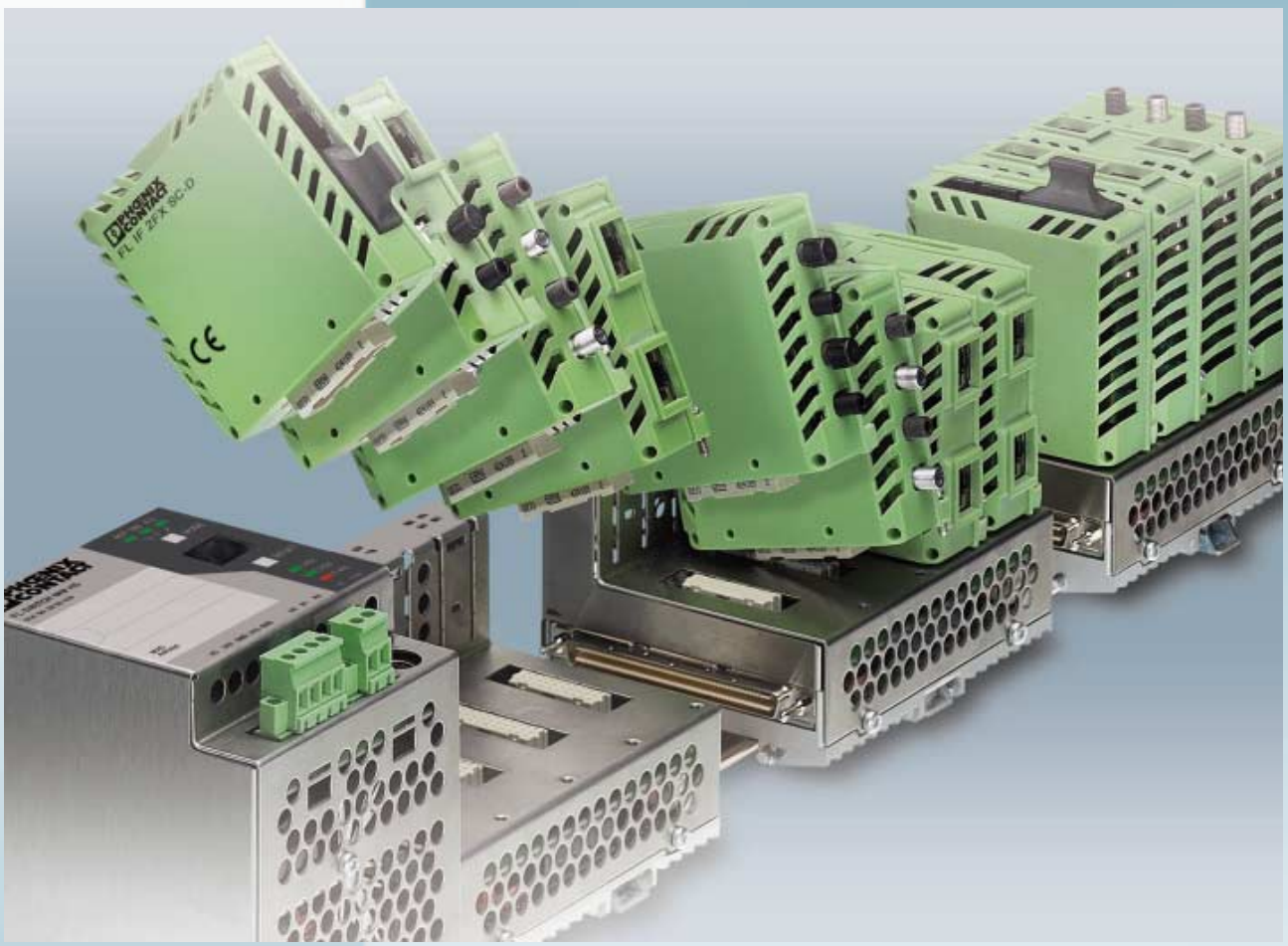
AUTOMATIONWORX



Anwenderhandbuch

FL SWITCH MM HS UM

Art.-Nr.: 2699008

Modular Managed Switch System

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATIONWORX

Anwenderhandbuch

Beschreibung der Hard- und Software-Funktionen des Modular Managed Switch System mit der Firmware-Version 4.60

07/2007

Bezeichnung: FL SWITCH MM HS UM

Revision: 10

Art.-Nr.: 2699008

Dieses Handbuch ist gültig für:

Das Modular Managed Switch System mit der Firmware-Version 4.60 der Factory Line Produktfamilie.
Zum Modular Managed Switch System gehören:
- die Kopfstationen FL SWITCH MM HS und FL SWITCH MM HS/M
- die Erweiterungsmodule FL MXT und FL MXT/M
- die verschiedenen Interface-Module FL IF ...

Bitte beachten Sie folgende Hinweise

Damit Sie das in diesem Handbuch beschriebene Produkt sicher einsetzen können, lesen und beachten Sie bitte dieses Handbuch aufmerksam. Die folgenden Hinweise geben Ihnen eine erste Orientierung zum Gebrauch des Handbuchs.

Zielgruppe des Handbuches

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen, die mit den geltenden nationalen Normen und sonstigen Vorschriften zur Elektrotechnik und insbesondere mit den einschlägigen Sicherheitskonzepten vertraut sind.
Für Fehlhandlungen und Schäden, die an Produkten von Phoenix Contact und Fremdprodukten durch Missachtung der Informationen dieses Handbuchs entstehen, übernimmt Phoenix Contact keine Haftung.

Erklärungen zu den verwendeten Symbolen

Das Symbol *Achtung* bezieht sich auf Handlungen, die einen Schaden der Hard- oder Software oder Personenschaden (im indirekten Zusammenhang mit gefährlicher Prozessperipherie) zur Folge haben können.

Das Symbol *Hinweis* vermittelt Bedingungen, die für einen fehlerfreien Betrieb unbedingt beachtet werden müssen. Es weist außerdem auf Tipps und Ratschläge für den effizienten Geräteeinsatz und die Software-Optimierung hin, um Ihnen Mehrarbeit zu ersparen.

Das Symbol *Text* verweist Sie auf weiterführende Informationsquellen (Handbücher, Datenblätter, Literatur etc.) zu dem angesprochenen Thema, Produkt o. ä. Ebenso gibt dieser Text hilfreiche Hinweise zur Orientierung im Handbuch.

Ihre Meinung interessiert uns

Wir sind ständig bemüht, die Qualität unserer Handbücher zu verbessern.

Sollten Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden.

PHOENIX CONTACT GmbH & Co. KG
Documentation Services
32823 Blomberg
DEUTSCHLAND

Telefon +49 - (0) 52 35 - 3-00
Telefax +49 - (0) 52 35 - 3-4 20 21
E-Mail tecdoc@phoenixcontact.com

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Die Phoenix Contact GmbH & Co. KG behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern.

Der Erhalt von technischer Dokumentation (insbesondere von Datenblättern, Montageanleitungen, Handbüchern etc.) begründet keine weitergehende Informationspflicht der Phoenix Contact GmbH & Co. KG über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Anderslautende Vereinbarungen gelten nur, wenn sie ausdrücklich von der Phoenix Contact GmbH & Co. KG in schriftlicher Form bestätigt sind. Bitte beachten Sie, dass die übergebene Dokumentation ausschließlich eine produktbezogene Dokumentation ist.

Obwohl die Phoenix Contact GmbH & Co. KG stets mit der notwendigen Sorgfalt darum bemüht ist, dass die Informationen und Inhalte korrekt und auf dem aktuellen Stand der Technik sind, können die Informationen technische Ungenauigkeiten und/oder Druckfehler enthalten. Die Phoenix Contact GmbH & Co. KG gibt keine Garantien oder Zusicherungen in Bezug auf die Genauigkeit und Richtigkeit der Informationen.
Die Phoenix Contact GmbH & Co. KG übernimmt keine Haftung oder Verantwortung für Fehler oder Auslassungen im Inhalt der technischen Dokumentation (insbesondere Datenblätter, Montageanleitungen, Handbücher etc.).

Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden – soweit gesetzlich zulässig – ohne jegliche ausdrückliche, konkludente oder stillschweigende Mängelhaftung oder Garantie erteilt. Sie enthalten keinerlei Beschaffenheitsvereinbarungen, beschreiben keine handelsübliche Qualität und stellen auch nicht Eigenschaftszusicherungen oder Zusicherungen im Hinblick auf die Eignung zu einem bestimmten Zweck dar.
Die Phoenix Contact GmbH & Co. KG behält sich das Recht vor, die Informationen und die in diesen Informationen beschriebenen Produkte jeder Zeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern.

Erklärungen zu den rechtlichen Grundlagen

Dieses Handbuch ist einschließlich aller darin enthaltenen Abbildungen urheberrechtlich geschützt. Jede Drittverwendung dieses Handbuchs ist verboten. Die Reproduktion, Übersetzung und öffentliche Zugänglichmachung sowie die elektronische und fotografische Archivierung und Veränderung bedarf der schriftlichen Genehmigung der Firma Phoenix Contact. Zuwiderhandlungen verpflichten zu Schadenersatz.

Phoenix Contact behält sich jegliche Änderungen, die dem technischen Fortschritt dienen, vor.

Alle Rechte für den Fall der Patenterteilung oder Gebrauchsmustereintragung sind Phoenix Contact vorbehalten. Fremdprodukte werden stets ohne Vermerk auf Patentrechte genannt. Die Existenz solcher Rechte ist daher nicht auszuschließen.

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact finden Sie im Internet unter:

www.phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:

www.download.phoenixcontact.de.

Inhaltsverzeichnis

1 Modular Managed Switch System 1-1

1.1 Eigenschaften 1-1
1.1.1 Systemkomponenten 1-3
1.1.2 Firmware-Versionen mit ihren Funktionen 1-5
1.1.3 Firmware-Funktionen und die erforderliche Hardware 1-7
1.1.4 Maße des Modular Managed Switch System im Normal-Betrieb 1-10
1.1.5 Maße des Modular Managed Switch System im nach GL zertifizierten Betrieb 1-11
1.1.6 Zuordnung der Ports zu den Steckplätzen 1-11
1.2 Status- und Diagnose-Anzeigen 1-12
1.2.1 LEDs der Kopfstation und der Erweiterungsmodule 1-12
1.2.2 Bedeutung der 7-Segment-Anzeige 1-14

2 Montage und Installation 2-1

2.1 Montage und Demontage der Kopfstation 2-1
2.2 Montage und Demontage der Erweiterungsmodule 2-3
2.3 Montage und Demontage der Interface-Module 2-5
2.4 Montage und Demontage des Beschriftungsfeldes FL M LABEL (Zubehör) 2-7
2.4.1 Montage 2-7
2.4.2 Demontage 2-8
2.4.3 Maße des Beschriftungsfeldes 2-8
2.5 Installation des Modular Managed Switch System 2-9
2.5.1 Anschließen der Versorgungsspannung an die Kopfstation FL SWITCH MM HS 2-9
2.5.2 Anschluss der Versorgungsspannung an den FL SWITCH MM HS/M für den nach GL zertifizierten Betrieb 2-10
2.5.3 Meldekontakt 2-11
2.5.4 V.24-Schnittstelle für externes Management 2-12
2.6 Erdung 2-12

3 Inbetriebnahme und Funktionen 3-1

3.1 Grundeinstellung 3-1
3.1.1 Auslieferungszustand / Werkseinstellungen 3-1
3.1.2 Vergabe der IP-Parameter 3-2
3.1.3 Ablaufdiagramm nach Neustart 3-7
3.2 Inbetriebnahme der Interface-Module 3-9
3.2.1 FL IF 2TX VS-RJ 3-9
3.2.2 FL IF 2POF 10/100 3-11
3.2.3 FL IF 2HCS 100 3-14
3.2.4 FL IF 2FX SC ... / FL IF 2FX SM SC 3-16

3.2.5 FL IF 2FX ST-D ... 3-18
3.2.6 FL IF TX/POF 10/100 3-19
3.2.7 FL IF TX/HCS 100 3-20
3.2.8 FL IF MEM 2TX-D / FL IF MEM 2TX-D/MRM ... 3-22
3.2.9 FL IF 2PSE-F ... 3-24
3.2.10 FL IF 2POF SCRJ-D ... 3-27
3.3 Frame-Switching ... 3-30
3.3.1 Store and Forward ... 3-30
3.3.2 Multiaddress-Fähigkeit ... 3-30
3.3.3 Adressen lernen ... 3-30
3.3.4 Priorisierung ... 3-31

4 Konfiguration und Diagnose ... 4-1
4.1 Factory Manager ... 4-1
4.1.1 Allgemeine Funktion ... 4-1
4.1.2 Vergabe der IP-Parameter ... 4-1
4.1.3 Konfiguration und Diagnose ... 4-3
4.2 Web Based Management - WBM ... 4-11
4.2.1 Allgemeine Funktion ... 4-11
4.2.2 Voraussetzungen für die Verwendung des WBM ... 4-11
4.2.3 Funktionen / Informationen im WBM ... 4-12
4.3 Simple Network Management Protocol - SNMP ... 4-41
4.3.1 Allgemeine Funktion ... 4-41
4.3.2 Schematische Darstellung von SNMP-Management ... 4-44
4.3.3 RFC1213-MIB - MIB II ... 4-46
4.3.4 RMON-MIB (1.3.6.1.2.1.16) ... 4-53
4.3.5 Bridge-MIB (1.3.6.1.2.1.17) ... 4-59
4.3.6 pBridgeMIB (1.3.6.1.2.1.17.6) ... 4-61
4.3.7 qBridgeMIB (1.3.6.1.2.1.17.7) ... 4-62
4.3.8 rstp MIB (1.3.6.1.2.1.17.11) ... 4-65
4.3.9 IANAifType-MIB (1.3.6.1.2.1.30) ... 4-66
4.3.10 IF-MIB (1.3.6.1.2.1.31) ... 4-66
4.3.11 pnoRedundancy.mib ... 4-69
4.3.12 Private MIBs ... 4-70
4.4 Management über lokale V.24-Kommunikationsschnittstelle ... 4-121
4.4.1 Allgemeine Funktion ... 4-121
4.4.2 Funktionen des User Interfaces ... 4-122
4.4.3 Start mit defekter Software (Firmware) ... 4-125
4.5 Management über Telnet ... 4-128
4.5.1 Konfiguration des Telnet-Terminals ... 4-128
4.5.2 Funktionen des Telnet-Interfaces ... 4-128

5 (Rapid) Spanning Tree ... 5-1
5.1 Allgemeine Funktion ... 5-1

5.2 Inbetriebnahme von (R)STP 5-2
5.2.1 Einschalten von (R)STP auf allen beteiligten Switches 5-2
5.2.2 Verbindungsausfall - Beispiel 5-11
5.2.3 Mischbetrieb zwischen RSTP und STP 5-13
5.2.4 Topologie-Erkennung eines Rapid-Spanning-Tree-Netzwerkes (RSTP) 5-13
5.2.5 Projektierungshinweise zu Rapid Spanning Tree 5-16

6 Medien-Redundanz-Protokoll - MRP 6-1
6.1 Allgemeine Funktion 6-1
6.2 Die MRP-Lizenz 6-1
6.2.1 Netzwerkbeispiele 6-2
6.3 Freischalten der Webseiten zur Nutzung von MRP im WBM 6-4
6.4 Konfiguration von MRP 6-4
6.4.1 MRP General 6-4
6.4.2 MRP Configuration 6-5

7 Multicast Filtering 7-1
7.1 Grundlagen 7-1
7.2 Freischalten der Webseiten zum Multicast Filtering im WBM 7-1
7.3 Statische Multicast-Gruppen 7-1
7.3.1 Webseite „Current Multicast Groups“ 7-2
7.3.2 Anlegen von statischen Multicast-Gruppen 7-2
7.3.3 Vorgehensweise zum Anlegen einer Multicast-Gruppe 7-4
7.4 Dynamische Multicast-Gruppen 7-7
7.4.1 Internet Group Management Protocol - IGMP 7-7
7.4.2 Webseite „General Multicast Configuration“ 7-8

8 Virtual Local Area Network - VLAN 8-1
8.1 Grundlagen 8-1
8.2 Freischalten der VLAN-Webseiten im Web Based Management 8-1
8.2.1 Management VLAN-ID 8-2
8.2.2 Änderung der Management VLAN-ID 8-2
8.3 General VLAN Configuration 8-3
8.4 Current VLANs 8-4
8.4.1 Static VLANs 8-5
8.4.2 VLAN Port Configuration 8-6
8.4.3 VLAN Port Configuration Table 8-6
8.5 Einrichten von statischen VLANs 8-7
8.5.1 Dynamische Konfiguration 8-9
8.6 VLAN & (R)STP 8-9

9 Betrieb als PROFINET-Device 9-1

9.1 Vorbereitung des Switches für die PROFINET-Betriebsart 9-1

9.2 Switch als PROFINET IO-Device 9-2

9.2.1 Projektierung im Engineering-Werkzeug 9-2

9.2.2 Switch als PROFINET IO-Device projektieren 9-4

9.2.3 PROFINET-Blink-Funktion 9-5

9.2.4 Gerätetaufe 9-5

9.2.5 Betrieb im PROFINET-Umfeld 9-5

9.3 Alarme bei PROFINET 9-5

9.3.1 Alarme im WBM 9-6

9.4 Prozessdatenkommunikation 9-6

9.4.1 Control Word 9-6

10 LLDP - Link Layer Discovery Protocol 10-1

10.1 Grundlagen 10-1

10.2 Darstellung der Topologie in einem Engineering-Tool 10-4

11 DHCP Relay Agent 11-1

11.1 Aktivierung des DHCP Relay Agents 11-1

12 Technische Daten und Bestelldaten 12-1

12.1 Technische Daten 12-1

12.2 Typische Stromaufnahme - MMS (Beispiel) 12-5

12.3 Bestelldaten 12-7

12.4 Bestelldaten der nach GL zertifizierten Komponenten (GL-Zertifikat 24 2750 4 HH) 12-8

A Anhang: Stichwortverzeichnis A-1

1 Modular Managed Switch System

Alle Angaben in diesem Handbuch gelten immer, sofern es nicht ausdrücklich anders vermerkt ist, sowohl für die Geräte FL SWITCH MM HS und FL SWITCH MM HS/M als auch für die Geräte FL MXT und FL MXT/M.

1.1 Eigenschaften

Der **M**odular **M**anaged **S**witch (**Modular Managed Switch System - MMS**) ist ein industrietauglicher Ethernet-Switch und besteht aus einer Kopfstation, den Erweiterungsmodulen und den Interface-Modulen. Die Kopfstation und die Erweiterungsmodule enthalten die gesamte Ethernet-Switching-Technologie. Die Interface-Module bilden die Schnittstelle zur gewünschten Übertragungsphysik. Mit Hilfe eines Erweiterungsmoduls können Sie die Kopfstation von acht Ports auf 16 Ports erweitern, mit zwei Erweiterungsmodulen auf maximal 24 Ports. Über die verschiedenen Interface-Module können Sie das gewünschte Übertragungsmedium frei wählen.

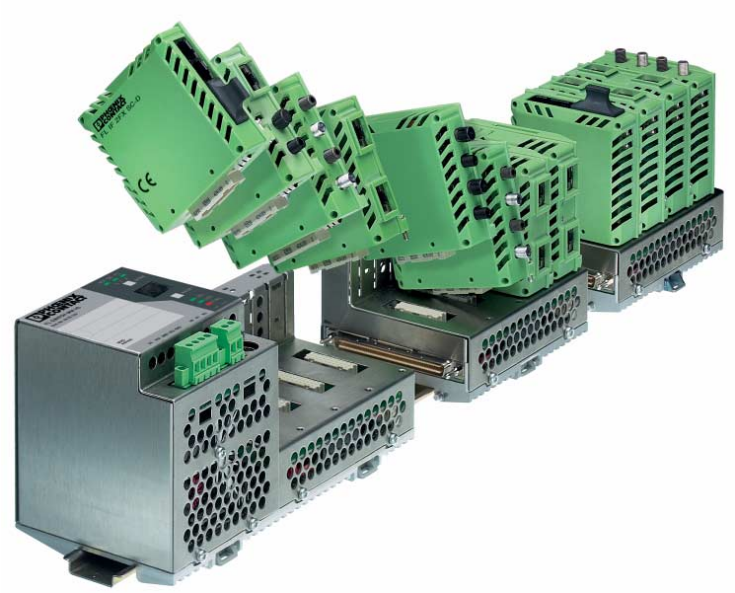


Bild 1-1 Das Modular Managed Switch System

Zukunftssichere Netze für höchste Ansprüche

Übertragungstechnik

10/100 MBit/s Polymer-/HCS-Faser
Endlich kann die einfach zu konfektionierende Polymerfaser auch für Ethernet verwendet werden. Überbrücken Sie Entfernungen von bis zu 50 m mit der preiswerten LWL-Technologie. Nutzen Sie die Kostenvorteile sowohl bei der Installation, als auch bei der Instandsetzung, wenn mechanisch beschädigte LWL-Leitungen ersetzt werden müssen.
Für Entfernungen von bis zu 100 m steht Ihnen die HCS-Faser-Technologie zur Verfügung.

Höchste Verfügbarkeit

Höchste Netz-Verfügbarkeit
Das lüfterlose Gerätedesign, die redundante Spannungsversorgung und die Einhaltung aller relevanten Industrie-Normen zu EMV, Klima, mechanischer Belastung etc. tragen zu höchster Verfügbarkeit bei.
Schaffen Sie Redundanz mit Standards: das (Rapid) Spanning Tree Protocol sorgt für den sicheren Betrieb des gesamten Netzwerkes in jeder Topologieform, auch dann, wenn eine Leitungsunterbrechung vorliegt.

Alle Informationen

Klare Informationen
Kennzeichnen Sie Ihr Gerät eindeutig auf dem großen Beschriftungsfeld, lesen Sie Betriebszustände und ergänzende Informationen auf der zweistelligen 7-Segment-Anzeige ab. Durch zwei LEDs pro Port mit umschaltbarer Information sind Sie auch „vor Ort“ immer ausreichend informiert. Für Diagnose/Wartung/Konfiguration über das Netzwerk steht Ihnen ein Webserver und ein SNMP-Agent zur Verfügung. Ein Terminal-Zugang kann für die Vor-Ort-Bedienung genutzt werden.

Port-Mirroring

Datenverkehr auf den Netzwerkverbindungen können Sie mittels Port-Mirroring überwachen.

Modularität

Modularer Aufbau
Stellen Sie bedarfsgerecht einen kompakten Switch für den Schaltschrank zusammen (mit komfortablen Anschlüssen nach vorne) oder einen Switch für den Klemmkasten (dann mit den Anschlüssen nach unten). Ergänzen Sie bei Bedarf eine Glasfaser-Schnittstelle oder erweitern Sie Ihre bestehende Station um acht / 16 Ports auf maximal 24 Ports.

Bild 1-2 Möglicher Hardware-Aufbau des Systems

Merkmale und Einsatzgebiete des FL SWITCH MM HS

- Steigerung der Netzperformance durch Filterung des Datenverkehrs:
  - Lokaler Datenverkehr bleibt lokal und
  - das Datenaufkommen in den Netzsegmenten wird reduziert.
- Einfache Netzerweiterung und Netzkonfiguration.
- Kopplung von Segmenten mit unterschiedlichen Übertragungsraten. Automatische Erkennung der Datenübertragungsrate von 10 MBit/s oder 100 MBit/s mit Autocrossing.
- Erhöhung der Verfügbarkeit durch Verwendung redundanter Übertragungswege mit Rapid Spanning Tree. Unterstützung verschiedener Topologieformen und vermaschten Strukturen sowie bei Ringtopologien mit spezieller Ringerkennung. Schnelle Umschaltzeiten mit RSTP Fast Ring Detection.
- Konfiguration des Switches über Web Based Management, SNMP, Telnet oder lokal über eine V.24-Schnittstelle.
- Multicast Filtering (statisch und dynamisch).
- IGMP Snooping, optionale Querier-Funktion.
- VLAN-Support nach 802.1Q (32 VLANs).
- Port Security-Funktionen.
- Zugriffsschutz auf das Web Based Management (WBM).
- Einbindung in PROFINET-Umgebungen.
- Topologie-Erkennung mit LLDP (Link Layer Discovery Protocol).
- Addressvergabe per BootP, DHCP, DCP oder statisch.
- Adressvergabe mit DHCP Option 82 Relay Agent.
- Unterstützung von Power-over-Ethernet (PoE).
- Unterstützung des Medien-Redundanz-Protokolls (MRP), sowohl als Client, als auch als Manager (in Verbindung mit dem Interface-Modul „FL IF MEM 2TX-D/MRM“). Dabei kann der MRP-Ring über beliebige Ports des MMS aufgebaut werden.

1.1.1 Systemkomponenten

Zentrales Element FL SWITCH MM HS

Die Kopfstation ist das zentrale Element des Modular Managed Switch Systems. Sie beinhaltet die gesamte Management-Funktionalität und erhält durch die Interface-Module die gewünschten Schnittstellen zum Netzwerk. An eine Kopfstation sind bis zu zwei Erweiterungsmodule anschließbar, so dass das System im Maximalaufbau 24 Ethernet-Ports umfasst.

FL SWITCH MM HS/M

Durch die Zertifizierung nach Germanischer Lloyd (GL-Zertifikat Nr. 2427504 HH) ist die Kopfstation FL SWITCH MM HS/M, das Erweiterungsmodul FL MXT/M und ein Teil der verfügbaren Interface-Module sowohl für den Schiffsbau, als auch für den Einsatz im Off-/Onshore-Bereich freigegeben. Beachten Sie die Liste der nach GL zertifizierten Komponenten auf Seite 12-8. Bitte beachten Sie außerdem die Hinweise zum Anschluss der Versorgungsspannung auf Seite 2-10.

Schalten Sie vor dem Hinzufügen und Entfernen von Erweiterungsmodulen (FL MXT) die Versorgungsspannung ab.

Schließen Sie nicht mehr als zwei Erweiterungsmodule (FL MXT) an eine Kopfstation an.

Erweiterungsmodul FL MXT

Ein Erweiterungsmodul stellt Ihnen weitere acht Ports zur Verfügung, die Sie individuell mit Interface-Modulen bestücken können. An die Kopfstation können maximal zwei Erweiterungsmodule angeschlossen werden. Im Maximalausbau stehen dann 24 Ports zur Verfügung.

Ein Betrieb der Erweiterungsmodule ohne die Kopfstation ist nicht möglich.

FL MXT/M

Das Erweiterungsmodul FL MXT/M ist aufgrund der Zertifizierung nach GL (Zertifikat Nr. 2427504 HH) sowohl für den Schiffsbau, als auch für den Einsatz im Off-/Onshore-Bereich freigegeben.

Interface-Module FL IF ...

Beachten Sie die Liste mit den nach GL zertifizierten Komponenten auf Seite 12-8.

Interface-Module bilden die gewünschte Schnittstelle zum Netzwerk. Durch die beiden Abgangsrichtungen, die verschiedenen Medientypen und die Portdichte von zwei Ports pro Interface-Modul ist ein höchst flexibler Aufbau des Systems möglich.

Converter Board FL CB IF

In Verbindung mit dem Converter Board FL CB IF kann das Interface-Modul FL IF TX/POF-... als „Stand-Alone“ Medienkonverter benutzt werden.

Bild 1-3 Converter Board FL CB IF

1.1.2 Firmware-Versionen mit ihren Funktionen

Die Firmware-Version 1.03 bietet die Standard-Switch-Funktionen.

Die Firmware-Version 1.11 unterstützt zusätzlich den Redundanzmechanismus Spanning Tree.

Die Firmware 2.03 bietet folgende zusätzlichen Funktionen:

– Multicast-Filtermechanismen
– IGMP-Snooping und Querier-Funktion
– Unterstützung des Memory-Modules

Die Firmware 2.10 bietet folgende zusätzlichen Funktionen:

– Auto-Refresh verschiedener Seiten des WBM
– die Unterstützung der POF- und FX-Interface-Module
– die ausführliche Unterstützung und ein verbessertes Konfigurations-Handling des Memory-Modules
– Erweiterte Multicast-Filterung (Multicast-Sender werden erkannt und zu Multicast-Gruppen hinzugefügt)
– Erweiterte IGMP-Snooping- und IGMP-Query-Funktion (Switch liest passiv IGMP-Membership-Reports und legt entsprechende Multicast-Gruppen an und sendet zur Multicast-Gruppenbildung IGMP-Queries aus)
– Visualisierung der Port-Auslastung
– Port-Priorisierung

Die Firmware 3.04 bietet folgende zusätzlichen Funktionen:

– Unterstützung von VLANs
– Unterstützung von Rapid Spanning Tree
– Security-Optionen (Port-basierte Security und Zugriffsschutz auf WBM)
– Optimierung des Password-Konzepts
– Ereignistabelle (Protokollierung wichtiger Ereignisse)
– Darstellung MAC-Adresstabelle im WBM

Die Firmware 4.03 bietet folgende zusätzlichen Funktionen:

– Optimiertes Rapid Spanning Tree Protocol (RSTP) (Verbesserung der Umschaltzeiten)
– Fast Ring Detection
– Large Tree Support
– Unterstützung von LLDP-Topologieerkennung
– DHCP-Support
– DHCP mit Option 82 Relay Agent
– PROFINET-Device-Funktionalität und DCP
– Unterstützung Power over Ethernet (IEEE 802.3af)
– Vereinfachte Portkonfiguration
– IGMP-Query Version 1und 2

Die Firmware 4.50 bietet folgende zusätzlichen Funktionen:

– Unterstützung des POF-SCRJ-Interface-Moduls und der zugehörigen Diagnose
– SNMP-Traps einzeln abschaltbar
– VLAN des Managements kann eingestellt werden: VLAN-ID für das Management (Web, SNMP, Ping, IGMP Query) des Switches im Modus „Vlan Tagging“
– DHCP Relay Agent portbezogen abschaltbar

- PROFINET Alarme und Konfigurationsvergleich
- Fast Aging bei Link-Down
- Erweiterte LED-Diagnose (Identifikation des Switches im PROFINET-Umfeld und Erkennung des Status „Fehlende IP-Parameter nach Neustart“)
- PoE-Traps (bei Änderung des PoE-Status)
- Test-Traps zur Überprüfung der Kommunikation
- Löschen der MAC-Adresstabelle aus dem WBM und SNMP

Die Firmware 4.60 bietet folgende zusätzlichen Funktionen:

- Unterstützung des Medien-Redundanz-Protokolls, sowohl als Client, als auch als Manager
- Erweiterte PROFINET IO-Device-Funktionalität
- Es werden bis zu 128 Multicastgruppen unterstützt, davon bis zu 20 statische Gruppen

1.1.3 Firmware-Funktionen und die erforderliche Hardware

Tabelle 1-1 Funktionen und erforderliche Hardware

Funktion	Erforderliche Hardware der Kopfstation	Erforderliche Hardware der Erweiterungsmodule
Standard-Switch-Funktionen	Hardware-Version ≥ 3 (enthält Systembusversion 4.1)	Hardware-Version ≥ 2 (enthält Systembusversion 3.1)
Unterstützung des Memory-Moduls	Hardware-Version ≥ 4 (enthält Systembusversion 4.2)	Hardware-Version ≥ 2 (enthält Systembusversion 3.1)
Unterstützung des PoE-Moduls	Hardware-Version ≥ 6 (enthält Systembusversion 5.0)	Hardware-Version ≥ 4 (enthält Systembusversion 4.0)
Unterstützung des POF-SCRJ-Moduls	Hardware-Version ≥ 6 (enthält Systembusversion 5.0)	Hardware-Version ≥ 4 (enthält Systembusversion 4.0)
Unterstützung des MRP-Moduls	Hardware-Version ≥ 6 (enthält Systembusversion 5.0)	Hardware-Version ≥ 4 (enthält Systembusversion 4.0)

1.1.3.1 Frontansicht der Kopfstation

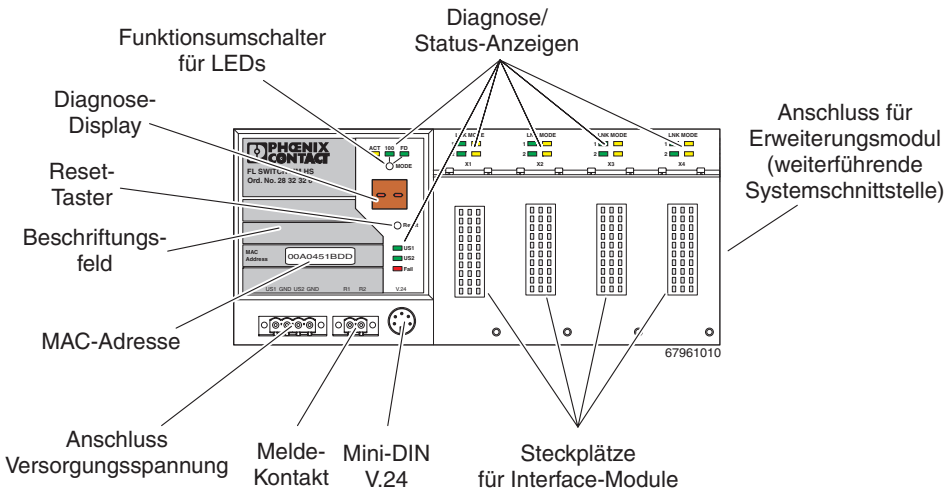


Bild 1-4 Frontansicht der Kopfstation

– Diagnose/Status-Anzeigen
  Wichtige Informationen werden direkt am Gerät dargestellt. Jeder Port besitzt zwei LEDs. Die linke LED zeigt stets den „LINK“ an, die Anzeige der rechten LED wird mit dem Funktionsumschalter eingestellt.
– Funktionsumschalter für LEDs
  Mit dem Umschalter (MODE) können Sie die Information, die die zweite portbezogene LED anzeigt, umschalten. Die drei LEDs oberhalb des Umschalters zeigen den gewählten Modus an. Diese Information wird dann von allen portbezogenen LEDs angezeigt (siehe auch Beispiel auf Seite 1-13).
– Anschluss für Erweiterungsmodul (FL MXT)
  Hier können Sie das erste von maximal zwei Erweiterungsmodulen anschließen.
– Steckplätze für Interface-Module
  Hier werden die verschiedenen Interface-Module (mit jeweils zwei Ports) aufgesteckt und arretiert.

– Mini-DIN V.24
  V.24-Schnittstelle im Mini-DIN-Format zur Konfiguration über die serielle Schnittstelle vor Ort.
– Meldekontakt
  Hier kann der potenzialfreie Meldekontakt über einen 2-poligen COMBICON-Stecker beschaltet werden.
– Anschluss Versorgungsspannung
  Über den 4-poligen COMBICON-Stecker kann die Versorgungsspannung angeschlossen werden (optional redundant).
– Reset-Taster

Um einen versehentlichen Reset des MMS zu vermeiden, muss der Reset-Taster einige Sekunden lang gedrückt werden, bevor der Reset ausgelöst wird.

– Diagnose-Display
  Verschiedene Betriebszustände oder Fehlerzustände können hier dargestellt werden. Eine Auflistung der möglichen Codes finden Sie auf Seite 1-14.

1.1.3.2 Frontansicht des Erweiterungsmoduls

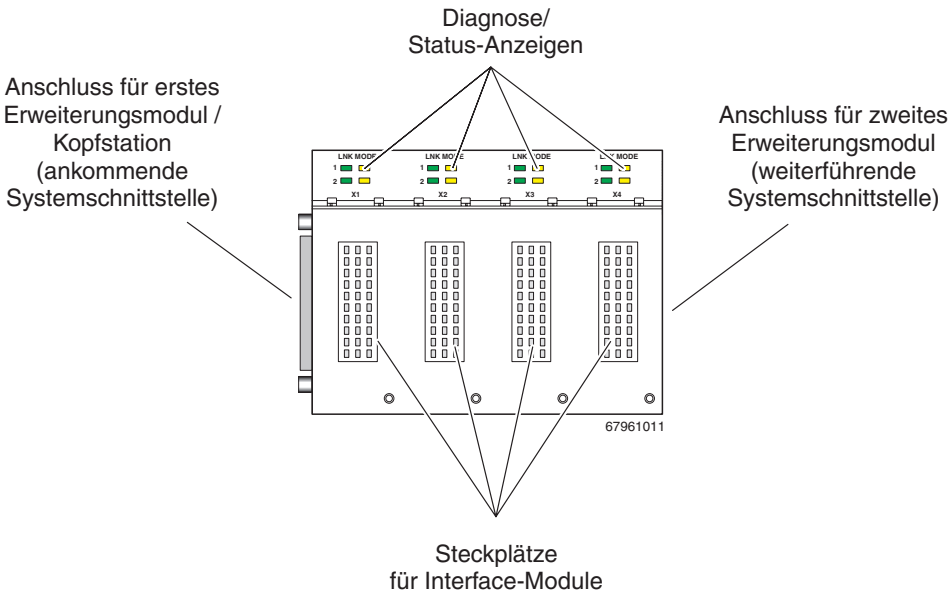


Bild 1-5 Frontansicht des Erweiterungsmoduls

– Diagnose/Status-Anzeigen
  Wichtige Informationen werden direkt am Gerät dargestellt.
– Anschluss für zweites Erweiterungsmodul
  Hier können Sie das zweite Erweiterungsmodul anschließen.
– Anschluss für Interface-Module
  Hier werden die verschiedenen Interface-Module aufgesteckt und arretiert.
– Steckplatz für erstes Erweiterungsmodul/Kopfstation
  Hier schließen Sie dieses Erweiterungsmodul entweder an eine Kopfstation oder an ein erstes Erweiterungsmodul an.

1.1.3.3 Ansicht der Interface-Module (Beispiel)

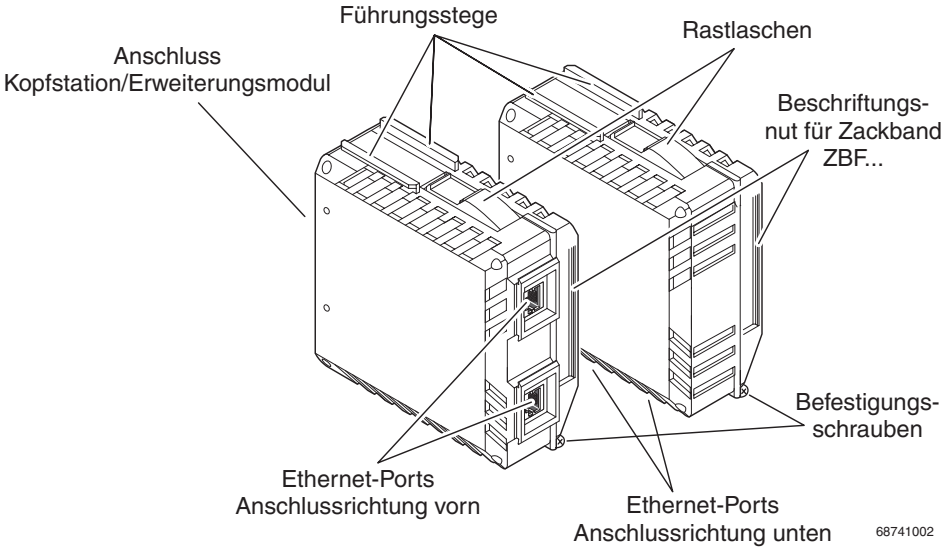
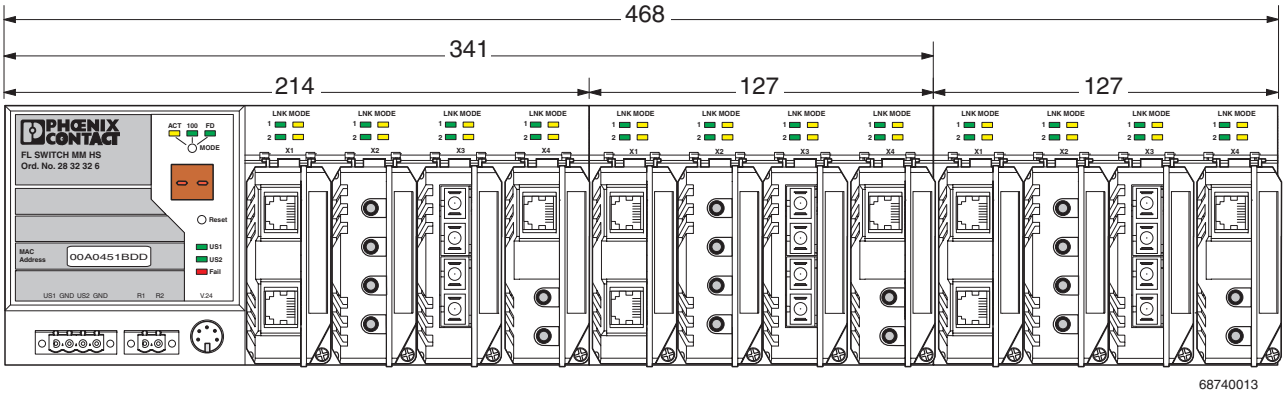


Bild 1-6 Ansicht der Interface-Module (Beispiel)

– Anschluss Erweiterungsmodul/Kopfstation
  Über diesen Stecker wird das Interface-Modul auf dem Erweiterungsmodul oder der Kopfstation kontaktiert.
– Führungsstege
  Diese Stege sorgen für einfache Montage und sicheren Halt der Interface-Module.
– Rastlaschen
  Nach dem Betätigen dieser Laschen kann das Interface-Modul wieder abgezogen werden (vorher Befestigungsschraube lösen).
– Ethernet-Ports
  Hier befinden sich die Ports der verschiedenen Schnittstellen und Anschlussrichtungen.
– Beschriftungsnut für Zackband ZBF ...
– Befestigungsschrauben zur Arretierung der Interface-Module.

1.1.4 Maße des Modular Managed Switch System im Normal-Betrieb



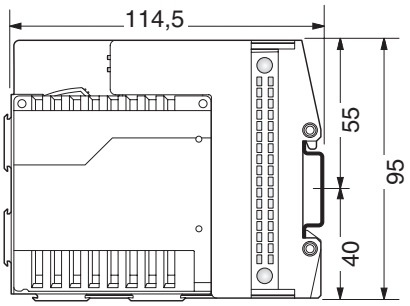
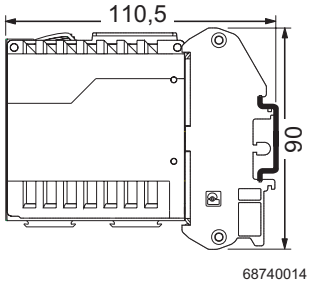


Bild 1-7 Gehäusemaße des MMS in Millimeter

Gehäusemaße des Converter Boards mit Interface-Modul



Gehäusebreite: 67 mm

Bild 1-8 Gehäusemaße des Converter Boards FL CB IF

1.1.5 Maße des Modular Managed Switch System im nach GL zertifizierten Betrieb

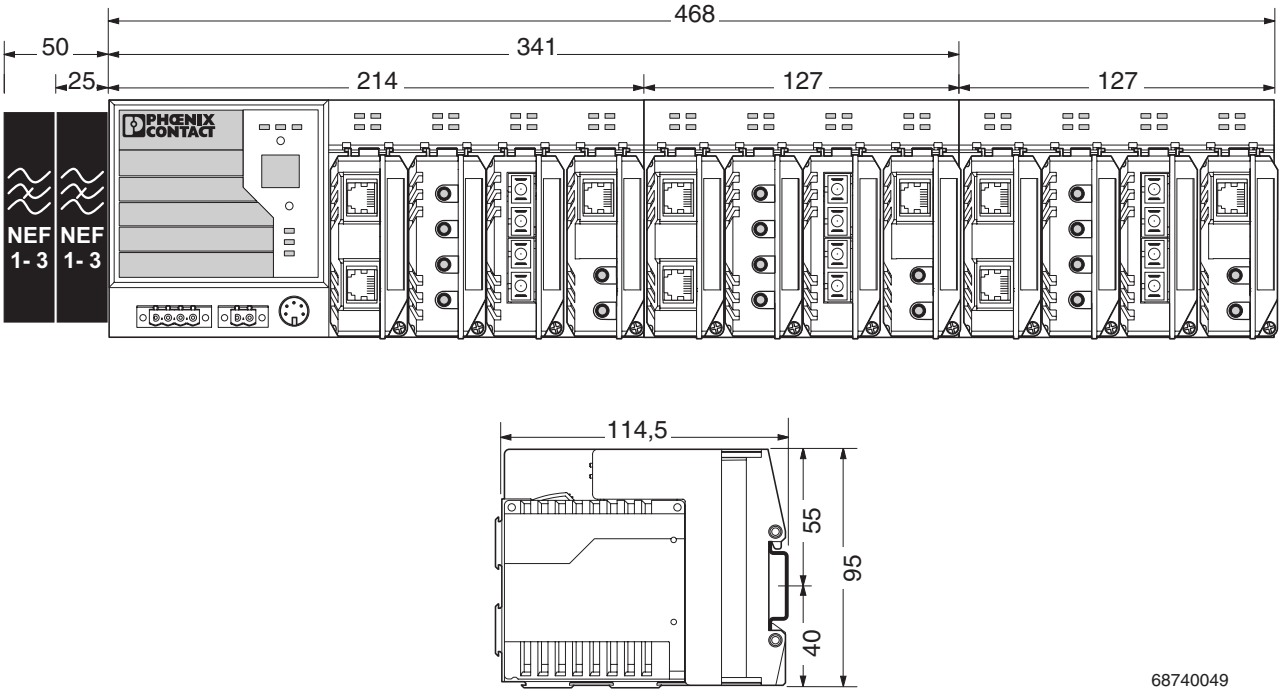


Bild 1-9 Gehäusemaße des MMS in Millimeter

1.1.6 Zuordnung der Ports zu den Steckplätzen

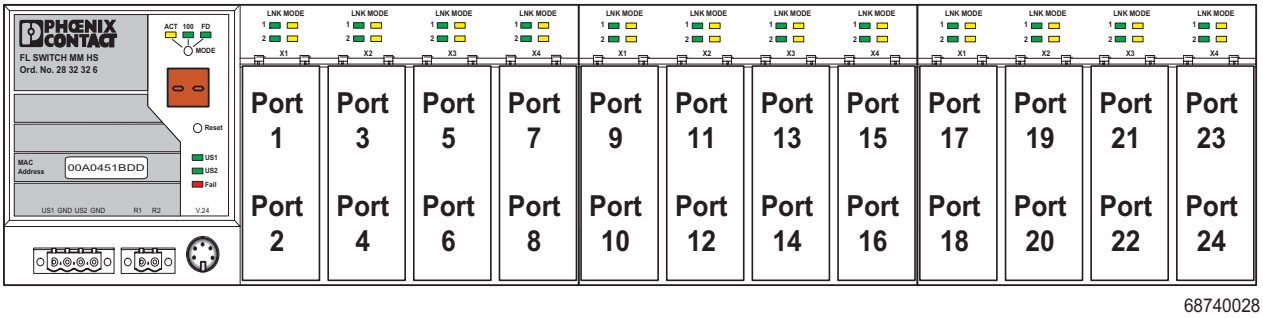


Bild 1-10 Zuordnung der Ports zu den Steckplätzen

1.2 Status- und Diagnose-Anzeigen

1.2.1 LEDs der Kopfstation und der Erweiterungsmodule

Bez.	Farbe	Status	Bedeutung
US1	grün	an	Versorgungsspannung 1 im Toleranzbereich
		aus	Versorgungsspannung 1 ist zu niedrig
US2	grün	an	Versorgungsspannung 2 im Toleranzbereich
		aus	Versorgungsspannung 2 ist zu niedrig
FAIL	rot	an	Meldekontakt offen, d. h. ein Fehler liegt vor
		aus	Meldekontakt geschlossen, d. h. ein Fehler liegt nicht vor
Für jeden Port befindet sich eine Link-LED oberhalb des Steckplatzes des Interface-Modules			
LNK (Link)	grün	an	Link aktiv
		aus	Link nicht aktiv
Für jeden Port befindet sich eine weitere LED oberhalb des Steckplatzes des Interface-Modules. Die Funktion der zweiten LED (MODE) je Port kann durch einen Schalter an der Kopfstation für alle Ports umgeschaltet werden (siehe auch nachfolgendes Beispiel). Drei Umschaltmöglichkeiten stehen zur Auswahl:			
ACT (Activity)	grün	an	Senden / Empfang von Telegrammen
		aus	Kein Senden / Empfang von Telegrammen
100	grün	an	100 MBit/s
		aus	10 MBit/s, wenn Link-LED aktiv
FD (Duplex)	grün	an	Full Duplex
		aus	Half Duplex, wenn Link-LED aktiv
ACT und 100 und FD gleichzeitig	grün	blinken	PROFINET-Geräteidentifikation
ACT oder 100 oder FD (durch Mode-Umschalter ausgewählt)	grün	blinken	Nach Neustart keine IP-Parameter vorhanden

Beispiel:

In Bild 1-11 haben die LED-Anzeigen folgende Bedeutung (siehe auch „Zuordnung der Ports zu den Steckplätzen“ auf Seite 1-11):

A: Mit dem Umschalter wurde der Duplex-Mode ausgewählt; die Mode-LEDs zeigen jetzt, dass Port 1 und Port 3 im Vollduplex-Mode und Port 2 und Port 4 im Halbduplex-Mode sind.

B: Mit dem Umschalter wurde die Datenübertragungsrate ausgewählt; die Mode-LEDs zeigen jetzt, dass Port 1 und Port 2 mit 10 MBit/s, Port 3 mit 100 MBit/s und Port 4 gar nicht betrieben werden.

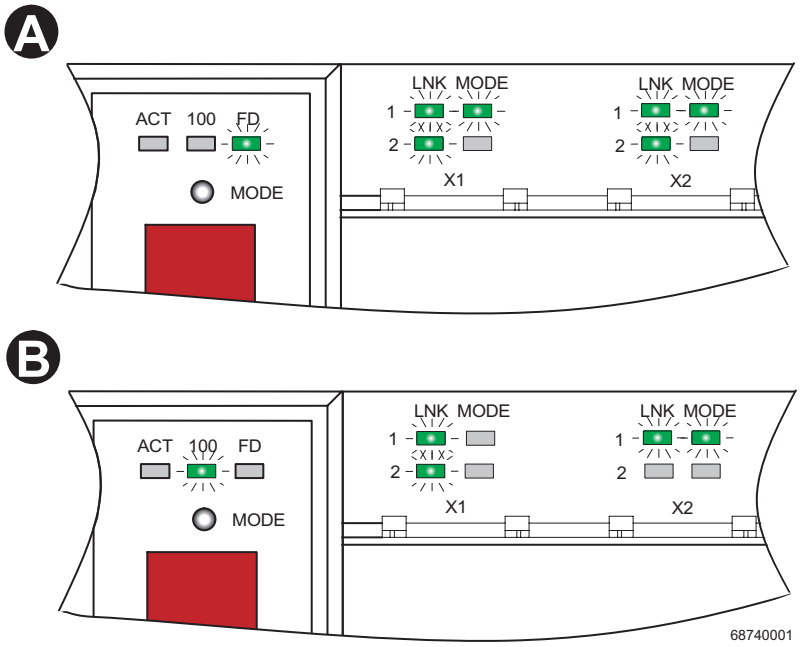
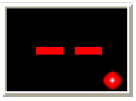


Bild 1-11 Beispiel für Status-Anzeigen

1.2.2 Bedeutung der 7-Segment-Anzeige



Wenn der MMS eine PROFINET-Verbindung aufgebaut hat, zeigt das Display unten rechts einen Punkt.

Im fehlerfreien Betrieb:

Anzeige	Bedeutung
bo	Entpacken/Start der Firmware (Boot)
01	Absenden der BootP-Requests
SC	Parametrierungsdaten werden im steckbaren Speicher und in der Kopfstation gespeichert
03	TFTP-Download der Firmware wird durchgeführt
04	Die über das Netzwerk geladene Firmware wird ins Flash geladen
05	Die neu geladene Firmware wurde erfolgreich ins Flash gespeichert
_ _	Initialisierung der Firmware
--	Firmware läuft
rb	Über SNMP, WBM oder V.24 wurde ein Reset ausgelöst, das Gerät bereitet den Neustart vor (Reboot)
rC	Nach einem Update der Gerätekonfiguration, kann nach einem Neustart „**rC**“ (Reconfiguration) im Display erscheinen. Das bedeutet, dass die Firmware selbstständig eine Anpassung der neuen Konfiguration vornimmt und dann nochmals einen Neustart des Switches durchführt.
Pb	Ein durch die Port-Security-Funktion geblockter Port wird mit „Pb“ angezeigt
dP	Das Gerät wird als PROFINET IO-Device betrieben und wartet auf die Inbetriebnahme durch einen PROFINET-Controller. Das Gerät ist nicht über eine IP-Adresse zu erreichen.
„00“ im Wechsel mit einer anderen Anzeige	Im PROFINET-Modus wurde durch das Engineering-Werkzeug die Funktion „Blinken“ aufgerufen.
SP	Spanning-Tree-Initialisierung aktiv

Meldungen beim Betrieb mit Memory-Modul:

Anzeige	Bedeutung
0P	Parametrierungsdaten werden vom steckbaren Speicher gelesen
EC	Equal Configuration - die Konfigurationen auf dem Memory-Modul und in der Kopfstation sind identisch
dC	Different Configuration - die Konfigurationen auf dem Memory-Modul und in der Kopfstation sind unterschiedlich
0C	Das Memory-Modul ist leer.

Meldungen beim Betrieb mit MRP-Memory-Modul:

Anzeige	Bedeutung
LF	Loop Failure - der MRP-Manager hat einen Fehler im redundanten Ring detektiert

Im Fehlerfall:

Anzeige	Bedeutung	Abhilfe
16	Die Software des Gerätes (Firmware) ist defekt	– Führen Sie ein Firmware-Update über die serielle Schnittstelle durch.
17	Die Übertragung der Firmware per TFTP oder Xmodem ist fehlgeschlagen (Wechsel der Anzeige von „03“ auf „17“)	– Prüfen Sie die physikalische Verbindung. – Stellen Sie eine Punkt-zu-Punkt-Verbindung her. – Stellen Sie sicher, dass die Datei (mit dem angegebenen Dateinamen) existiert und sich im richtigen Verzeichnis befindet. – Prüfen Sie die IP-Adresse des TFTP-Servers. – Aktivieren Sie den TFTP-Server. – Wiederholen Sie den Download.
19	Die Übertragung der Datei wurde erfolgreich abgeschlossen, aber die Datei ist keine gültige Firmware für das Modular Managed Switch System	– Stellen Sie eine gültige Firmware mit dem zuvor angegebenen Dateinamen zur Verfügung (Internet: www.phoenixcontact.com). – Wiederholen Sie den Download.
80	In der Firmware ist ein Fehler aufgetreten	– Starten Sie das Gerät neu (Power Up oder Reset). – Stellen Sie sicher, dass die verwendete IP-Adresse nicht mehrfach im selben Netz verwendet wird.
87	Mehr als ein Parametrierungsspeicher gesteckt	– Entfernen Sie alle Memory-Module bis auf eines und führen Sie einen Reset durch.
89	Der Switch ist oder war in einer Ausnahmesituation	– Führen Sie einen Neustart des Gerätes durch. – Überprüfen Sie Ihr Netzwerk auf Fehlkonfiguration, Loop-Bildung, Wackelkontakte, mangelnde Leitungsqualität, fehlerhafte Netzwerk-Interfaces. – Stellen Sie sicher, dass keine Denial-of-Service-Attacke stattfindet.
Li	Die Link-Überwachung hat mindestens einen fehlenden Link erkannt	– Überprüfen Sie die Leitungen/Stecker. – Überprüfen Sie im Web Based Management für welchen Port die Linküberwachung (siehe Seite 4-27) einen Fehler anzeigt. – Stellen Sie die Datenverbindung zu diesem Port wieder her oder deaktivieren Sie die Link-Überwachung für diesen Port. – Überprüfen Sie den korrekten Sitz des Interface-Moduls auf der Kopfstation oder auf dem Erweiterungsmodul.

Anzeige	Bedeutung	Abhilfe
Cd	Der Switch wird als PROFINET IO-Device betrieben. Die Konfiguration des Switches und die vom PROFINET-Engineering-Tool übertragene Konfiguration sind unterschiedlich	– Stellen Sie die gewünschte Konfiguration am Switch her. – Ändern Sie das Steuerungsprogramm so, dass es die vorhandene Switch-Konfiguration beinhaltet.
bF	Systembus-Fehler (Bus Fail)	– Stellen Sie sicher, dass die Erweiterungsmodule korrekt gesteckt sind. – Starten Sie den Switch neu.
Po	Power	– An mindestens einem Port wurde die Power-over-Ethernet-Überwachung aktiviert und ein Fehler liegt vor. Überprüfen Sie physikalische Verbindung an den PoE-Ports und die Einstellungen im WBM.
HS	Hardware Support	– Auf dem MMS ist mindestens ein Interface-Modul gesteckt, dass von der verwendeten MMS-Hardware-Version nicht vollständig unterstützt wird. Das Interface-Modul überträgt Daten, die Management-Funktionen sind deaktiviert. Die Meldung erscheint nach einem Neustart oder nach dem Stecken/Ziehen von Interface-Modulen für ca. zehn Sekunden im Display. Sie können das Interface-Modul unmanaged verwenden.
LF	Loop Failure - der redundante Ring ist unterbrochen	– Der redundante Ring ist physikalisch unterbrochen. Überprüfen Sie die physikalische Verbindung. – Der als Redundanzmanager konfigurierte Switch hat beim letzten Gerätestart kein gültiges Lizenzmodul gefunden, es ist keine redundante Verbindung gegeben. Stellen Sie sicher, dass genau ein Switch im MRP-Ring als MRP-Manager konfiguriert **und ein gültiges Lizenzmodul gesteckt** ist. – Falsche Ports. Stellen Sie sicher, dass der MRP-Ring nur über die Ports aufgebaut wird, die als MRP-Port konfiguriert sind. – Ungeeignete Switches. Stellen Sie sicher, dass alle Switches, die den MRP-Ring bilden, MRP unterstützen.

Die Punkte unter „Abhilfe“ sind Empfehlungen, die Sie nicht alle und nicht gleichzeitig durchführen müssen.

Bei allen nicht aufgeführten Meldungs-Codes kontaktieren Sie bitte Phoenix Contact.

2 Montage und Installation

2.1 Montage und Demontage der Kopfstation

Montieren/demontieren Sie die Kopfstation und die Erweiterungsmodule immer bei abgeschalteter Versorgungsspannung.

Montieren Sie die Kopfstation auf einer sauberen Tragschiene nach DIN EN 50 022 (z. B. NS 35 ... von Phoenix Contact). Verwenden Sie nur saubere korrosionsfreie Tragschienen, um Übergangswiderstände zu vermeiden. Um ein Verrutschen der Module auf der Tragschiene zu verhindern, sollten Sie vor der Montage der Module auf der linken Seite neben der Kopfstation einen Endhalter (E/NS 35N, Art-Nr. 08 00 88 6) montieren. Setzen Sie die mitgelieferte seitliche Abdeckung -ATP-ST-TWIN- (siehe „A“ in Bild 2-4) und den Endhalter auf der rechten Seite erst nach der Montage des letzten Erweiterungsmoduls.

Montage:

1. Setzen Sie das Modul von oben auf die Tragschiene (A). Dabei muss die obere Haltenut des Moduls mit der Oberkante der Tragschiene verhaken. Drücken Sie das Modul an der Front in Richtung der Montagefläche (B).

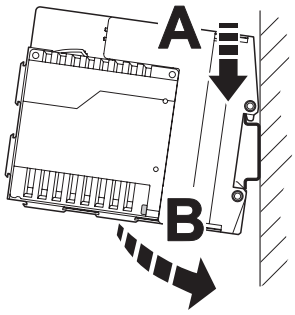


Bild 2-1 Aufrasten der Kopfstation auf die Tragschiene

2. Nachdem das Modul hörbar eingerastet hat, prüfen Sie den festen Sitz auf der Tragschiene. Überprüfen Sie, ob die Rastlaschen nach oben gerichtet, also eingerastet, sind.

Demontage:

1. Entfernen Sie alle Steckverbindungen oder die Interface-Module.
2. Ziehen Sie die Rastlaschen mit einem geeigneten Werkzeug (z. B. Schraubendreher) nach unten. Die beiden Rastlaschen verbleiben im ausgerasteten Zustand. Schwenken Sie dann die Unterseite des Moduls etwas von der Tragschiene weg (A). Heben Sie dann das Modul nach oben hin von der Tragschiene weg (B).

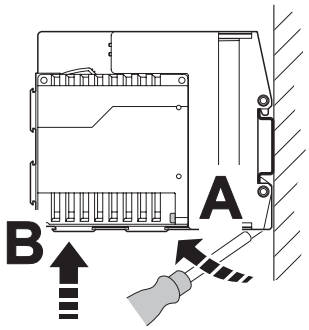


Bild 2-2 Demontage der Kopfstation

2.2 Montage und Demontage der Erweiterungsmodule

Montieren/demontieren Sie die Erweiterungsmodule immer bei abgeschalteter Versorgungsspannung.

Montage:

1. Setzen Sie das Modul von oben auf die Tragschiene (A). Dabei muss die obere Haltenut des Moduls mit der Oberkante der Tragschiene verhaken. Drücken Sie das Modul an der Front in Richtung der Montagefläche (B). Prüfen Sie die Verrastung der Rastlaschen.

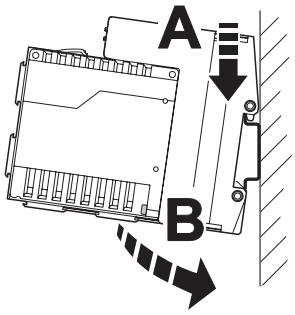


Bild 2-3 Montage der Erweiterungsmodule

2. Schieben Sie jetzt das auf der Hutschiene verrastete Erweiterungsmodul entlang der Tragschiene in Richtung der Kopfstation zusammen, bis die Stecker-/Buchsenleiste der Module ineinanderrasten und die Seitenteile der Module bündig aneinanderliegen.

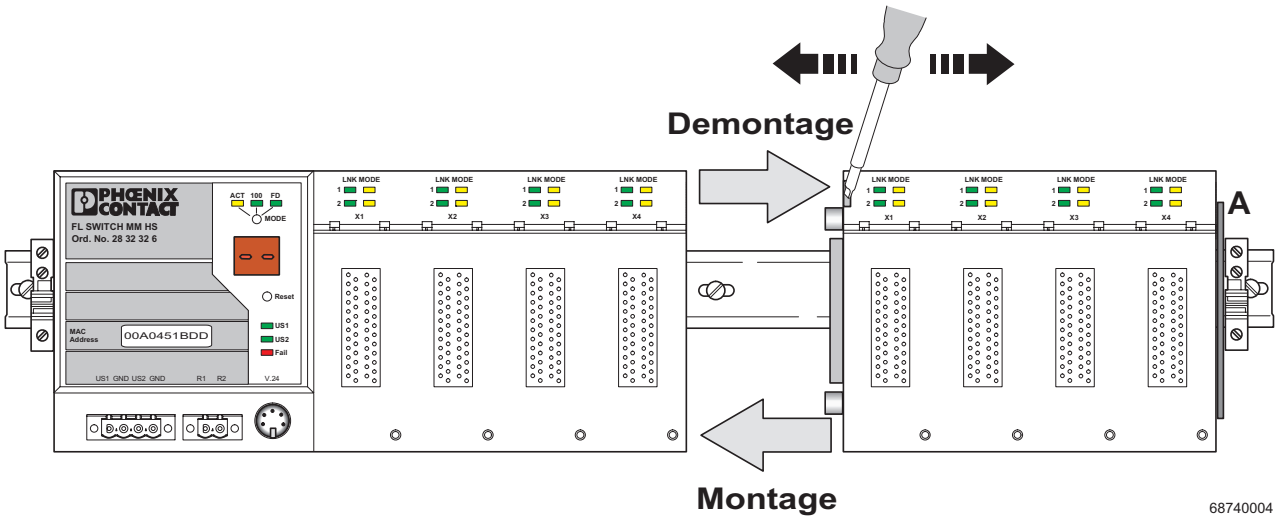


Bild 2-4 Montage/Demontage der Erweiterungsmodule

Demontage:

Schalten Sie vor der Demontage der Erweiterungsmodule die Versorgungsspannung ab.

1. Entfernen Sie alle Steckverbindungen oder die Interface-Module.
2. Um die Steckverbindung der Systemschnittstelle zu lösen, können Sie mit einem Schraubendreher die Module an der vorgesehen Kerbe auseinander drücken.
3. Schieben Sie das jeweils rechte Erweiterungsmodul nach rechts entlang der Tragschiene bis der Steckkontakt komplett frei liegt.
4. Ziehen Sie die Haltelaschen mit einem geeigneten Werkzeug (z. B. Schraubendreher) nach unten.
5. Schwenken Sie dann die Unterseite des Moduls etwas von der Tragschiene weg (A). Heben Sie dann das Modul nach oben hin von der Tragschiene weg.

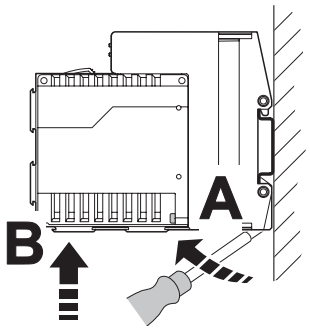


Bild 2-5 Demontage der Erweiterungsmodule

2.3 Montage und Demontage der Interface-Module

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

Stellen Sie sicher, dass die Oberfläche des Gehäuses der Kopfstation oder des Erweiterungsmoduls sauber ist.

Montage:

1. Stecken Sie die Interface-Module auf die Steckplätze der Grundmodule. Dabei müssen die Führungsstege auf der Oberseite der Interface-Module ohne zu Verkanten in die Führungsnuten am Grundmodul geschoben werden.

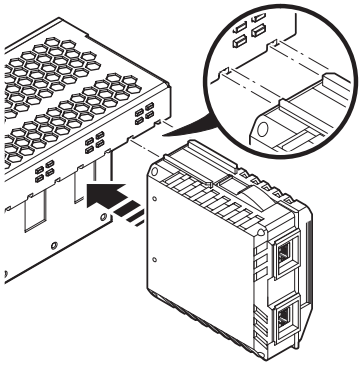


Bild 2-6 Montage der Interface-Module

2. Schieben Sie nun die Interface-Module in Richtung des Grundmoduls, bis der Stecker und die Haltespange eingerastet sind.
3. Sichern Sie das Interface-Modul mit der Schraube unten rechts am Interface-Modul.

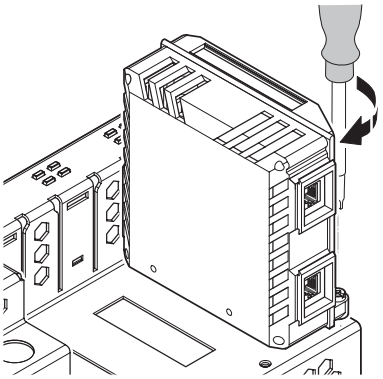


Bild 2-7 Sichern des Interface-Moduls

Demontage:

1. Lösen Sie die Befestigungsschraube.

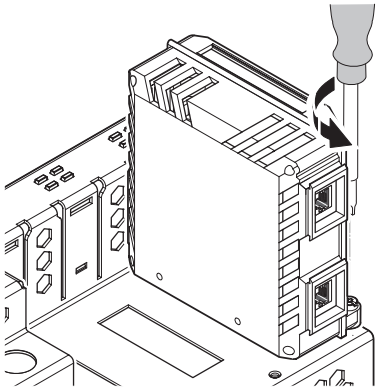


Bild 2-8 Lösen der Befestigungsschraube der Interface-Module

2. Drücken Sie die Rastlasche (A) und ziehen Sie das Modul ab (B).

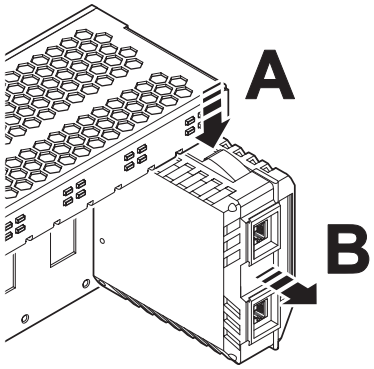


Bild 2-9 Entfernen des Interface-Moduls

2.4 Montage und Demontage des Beschriftungsfeldes FL M LABEL (Zubehör)

Mit dem Beschriftungsfeld FL M LABEL (Art.-Nr. 2891055) lassen sich die Ports des MMS individuell kennzeichnen. Das Beschriftungsfeld lässt sich auf der Oberseite der Kopfstation oder auf den Erweiterungsmodulen befestigen.

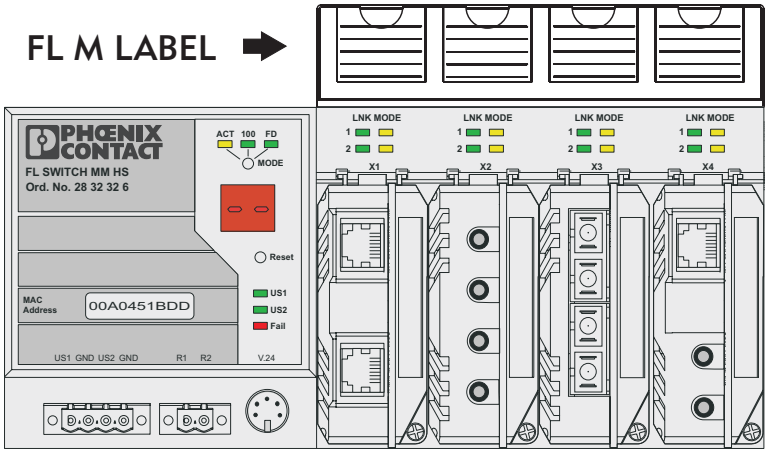


Bild 2-10 Kopfstation mit Beschriftungsfeld

2.4.1 Montage

– Stecken Sie die Spreizdübel durch die Befestigungslöcher des Beschriftungsfeldes und in die Öffnungen auf der Oberseite des MMS (A).
– Drücken Sie die Kappe des Spreizdübels herunter, um den Dübel zu befestigen (B).

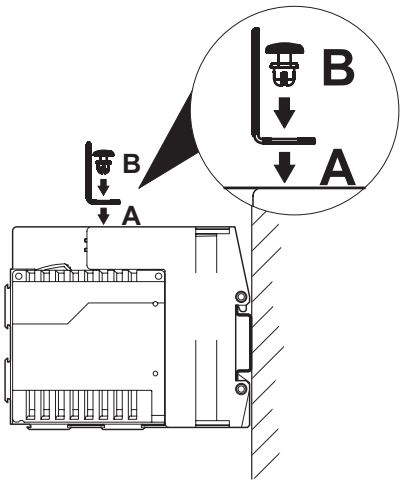


Bild 2-11 Montage des Beschriftungsfeldes

2.4.2 Demontage

– Ziehen Sie die Kappe des Spreizdübels nach oben bis der gesamte Dübel entfernt ist.
– Entfernen Sie das Beschriftungsfeld.

2.4.3 Maße des Beschriftungsfeldes

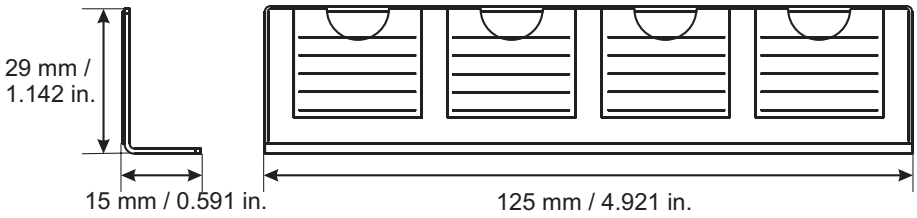


Bild 2-12 Maße des Beschriftungsfeldes

2.5 Installation des Modular Managed Switch System

2.5.1 Anschließen der Versorgungsspannung an die Kopfstation FL SWITCH MM HS

24 V DC

Das System wird mit einer 24-V-DC-Spannung betrieben, die an der Kopfstation angelegt wird. Bei Bedarf kann die Spannung redundant zugeführt werden (siehe Bild 2-14).

Falls die Überwachung der redundanten Spannungsversorgung aktiv ist (Default), wird ein Fehler gemeldet, falls nur eine Spannung zur Versorgung angelegt wird. Durch eine Brücke zwischen US1 und US2 (gestrichelte Verbindung) wird die Fehlermeldung vermieden. Sie können die Überwachung aber auch im Web Based Management oder über SNMP ausschalten.

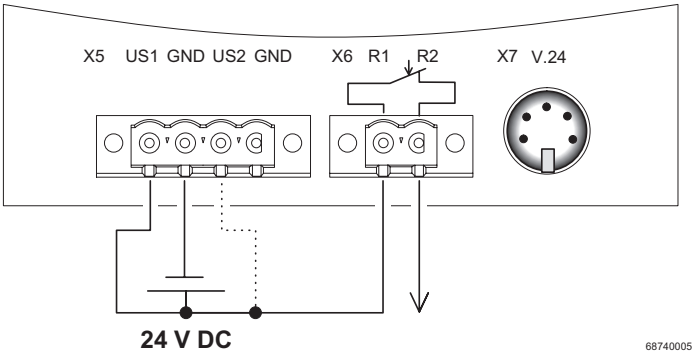


Bild 2-13 Versorgung des Systems mit einer Spannungsquelle

Redundante 24-V-DC-Einspeisung

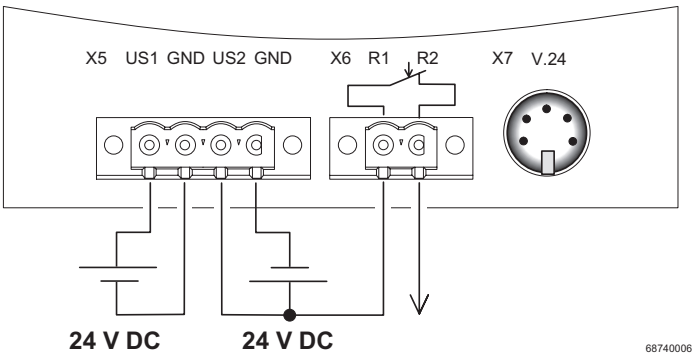


Bild 2-14 Versorgung des Systems mit zwei Spannungsquellen

2.5.2 Anschluss der Versorgungsspannung an den FL SWITCH MM HS/M für den nach GL zertifizierten Betrieb

Für einen nach GL zertifizierten Betrieb ist die Verwendung der Filter NEF 1- 3 (für Environmental Category EMC2) oder NEF 1- 6 (für EMC1) und der Einsatz in einem metallischen Schaltkasten zwingend vorgeschrieben.

24 V DC

Das System wird mit einer 24-V-DC-Spannung betrieben, die an der Kopfstation angelegt wird. Bei Bedarf kann die Spannung redundant zugeführt werden (siehe Bild 2-16).

Falls die Überwachung der redundanten Spannungsversorgung aktiv ist (Default), wird ein Fehler gemeldet, falls nur eine Spannung zur Versorgung angelegt wird. Durch eine Brücke zwischen US1 und US2 (gestrichelte Verbindung) wird die Fehlermeldung vermieden. Sie können die Überwachung aber auch im Web Based Management oder über SNMP ausschalten.

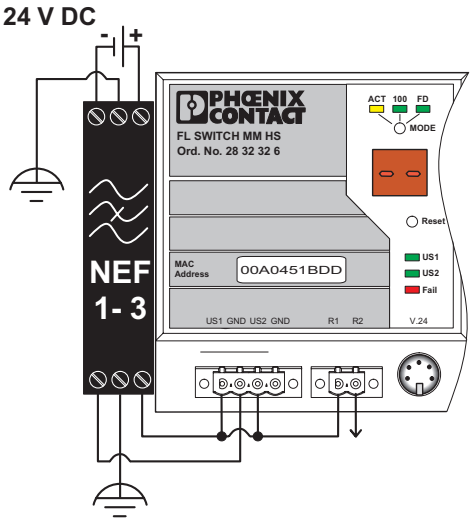


Bild 2-15 Versorgung des Systems mit einer Spannungsquelle

Redundante 24-V-DC-Einspeisung

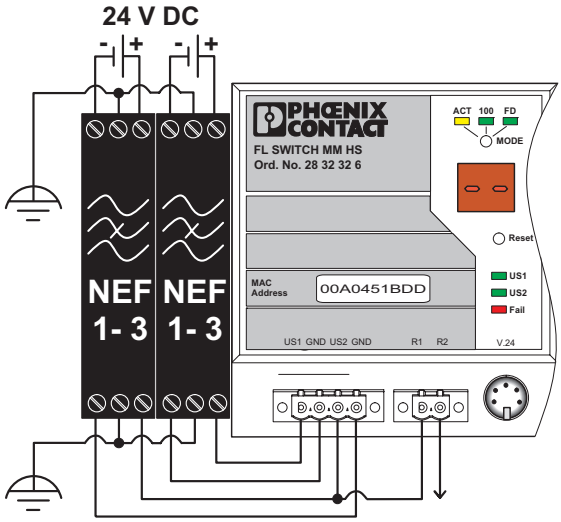


Bild 2-16 Versorgung des Systems mit zwei Spannungsquellen

2.5.3 Meldekontakt

Der Switch verfügt über einen potenzialfreien Meldekontakt. Durch Öffnen des Kontaktes wird ein Fehler gemeldet.

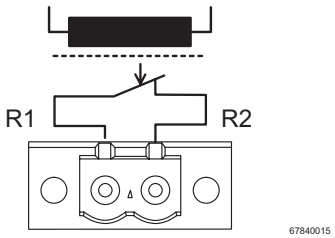


Bild 2-17 Prinzip-Schaltbild des Meldekontaktes

Die Konfiguration der gemeldeten Fehlerzustände erfolgt im Web Based Management oder über SNMP. Die konfigurierbaren Fehlerzustände finden Sie im Kapitel „Menü „Diagnostics\Alarm Contact““ auf Seite 4-37.

Bei nicht redundanter Spannungszuführung meldet der Switch durch Öffnen des Meldekontaktes den Ausfall einer Versorgungsspannung. Sie können diese Fehlermeldung verhindern, indem Sie, wie in Bild 2-13 oder Bild 2-15 (für GL) dargestellt, die Versorgungsspannung parallel auf beide Klemmen führen oder die Überwachung der redundanten Spannungsversorgung im Web Based Management deaktivieren.

2.5.4 V.24-Schnittstelle für externes Management

Über die sechspolige Mini-DIN-Buchse steht eine serielle Schnittstelle für den Anschluss einer lokalen Management-Station zur Verfügung. Damit kann über ein VT100-Terminal oder einen PC mit entsprechender Terminal-Emulation eine Verbindung zum Management-Interface hergestellt werden (ein entsprechendes Kabel finden Sie auf Seite 12-7). Stellen Sie folgende Übertragungsparameter ein:

Bits pro Sekunde	38400
Datenbits	8
Parität	Keine
Stoppbits	1
Flusssteuerung	Kein

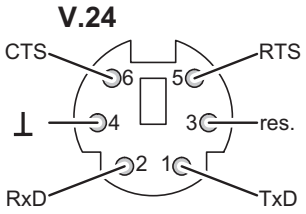


Bild 2-18 Übertragungsparameter und Belegung der V.24-Schnittstelle

2.6 Erdung

Eine Erdung dient dem Schutz von Menschen und Maschinen vor gefährlichen Spannungen. Um diese Gefahren so weit wie möglich auszuschließen, ist eine vorschriftsmäßige und den Gegebenheiten angepasste Erdung zwingend notwendig.

Alle Factory-Line-Teilnehmer müssen geerdet werden, damit mögliche Störungen vom Datentelegramm ferngehalten und auf Erdpotenzial abgeleitet werden können.

Die Erdung muss mindestens über einen 2,5-mm^2-Leiter erfolgen. Bei der Tragschienenmontage muss die Tragschiene über Erdungsklemmen mit der Schutzerde verbunden sein. Die Verbindung des Moduls zur Schutzerde erfolgt über das metallene Grundgehäuse.

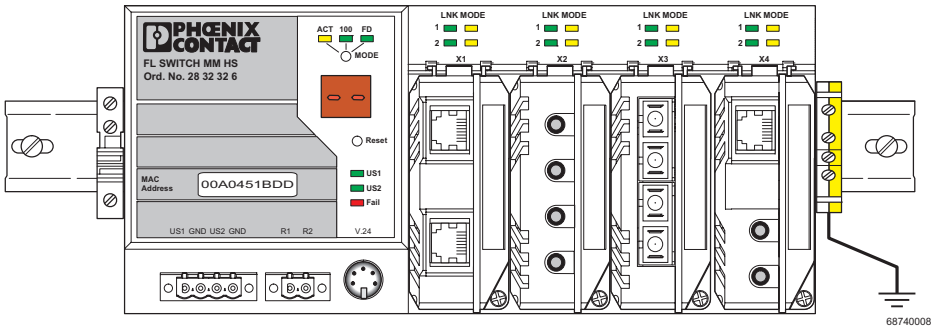


Bild 2-19 Switch auf geerdeter Tragschiene

3 Inbetriebnahme und Funktionen

3.1 Grundeinstellung

Die grundlegenden Ethernet-Funktionen sind ohne Konfiguration nach dem Zuschalten der Versorgungsspannung verfügbar.

3.1.1 Auslieferungszustand / Werkseinstellungen

Im Auslieferungszustand oder nach einem späteren Rücksetzen auf die Werkseinstellungen sind folgende Funktionen und Eigenschaften vorhanden:

– Das Passwort lautet: „private“.
– Alle IP-Parameter sind gelöscht. Der Switch verfügt über **keine** gültigen IP-Parameter:
  IP-Adresse: 0.0.0.0
  Subnetzmaske: 0.0.0.0
  Gateway: 0.0.0.0
– BootP ist als Adressierungsmechanismus aktiviert.
– Alle vorhandenen Ports sind mit folgenden Parametern aktiviert:
  - Autonegotiation bzw.
  - 100 MBit/s - vollduplex bei FX-Glasfasermodulen und HCS-Ports.
– Alle Zähler des SNMP-Agents sind gelöscht.
– Web- und Telnetserver, SNMP-Agent und V.24-Schnittstelle sind aktiv.
– Port Mirroring, Rapid Spanning Tree, Access Control for Web Interface, Port Security, Multicast-Filtering, VLAN, DHCP Relay Agent Option 82, LLDP und MRP sind deaktiviert.
– Port Security ist für alle Ports deaktiviert.
– Zugriffsschutz auf WBM ist deaktiviert.
– Der Alarm-Kontakt öffnet nur bei nicht-redundanter Spannungsversorgung und bei einem detektierten PoE-Fehler.
– Das Senden von SNMP-Traps ist deaktiviert und der Switch verfügt über keine gültige Trap-Destination-IP-Adresse
– Die Aging Time ist auf 40 Sekunden eingestellt.
– Der Switch befindet sich in der Betriebsart „Normal“.
– Aktualisierungs-Intervall des WBM ist auf 30 Sekunden eingestellt.
– Das Management befindet sich in VLAN 1.

Die Aging-Time wird über das MIB-Objekt „dot1dTpAgingTime“
(OID 1.3.6.1.2.1.17.4.2) eingestellt. Der mögliche Einstellbereich beträgt 10 - 825 Sekunden. Bei statischer Konfiguration wird eine Aging-Time von 300 Sekunden empfohlen.

Ein gestecktes Memory-Modul wird beim Neustart des Switches mit der aktuellen Konfiguration inkl. IP-Parameter beschrieben.

3.1.2 Vergabe der IP-Parameter

Nach dem Einschalten der Versorgungsspannung oder nach Betätigen des Reset-Tasters sendet der Switch Anfragen (BootP-Requests) zur Erteilung der IP-Parameter.

Zum Auslösen eines Resets muss der Taster einige Sekunden lang gedrückt werden.

Die Funktion „BootP“ kann über das Management deaktiviert sein. Im Auslieferungszustand ist die Funktion „BootP“ aktiviert.

Die Vergabe von gültigen IP-Parametern ist für die Management-Funktion des Switches unbedingt erforderlich.

Solange der Switch keine gültigen IP-Parameter erhalten hat, wird im Display „01“ oder „dc“ angezeigt und eine der Mode-LEDs (ACT, 100 oder FD) blinkt.

Möglichkeiten der Vergabe von IP-Parametern:

– Konfiguration über das BootP-Protokoll (Lieferzustand),
– Statische Konfiguration über die Management-Interfaces,
– DHCP (Dynamic Host Configuration Protocol) oder
– DCP (Discovery and Configuration Protocol)

In Kapitel 4.1.2 auf Seite 4-1 ist die Vergabe der IP-Parameter mit Factory Manager 2.1 beschrieben.

3.1.2.1 Gültige IP-Parameter

Die drei Elemente „IP-Adresse“, „Subnetz-Maske“ und „Default Gateway/Router“ bilden die IP-Parameter.

Gültige IP-Adressen sind:
000.000.000.001 bis 126.255.255.255 und
128.000.000.000 bis 223.255.255.255

Gültige Multicast-Adressen sind:
224.000.000.001 bis 239.255.255.255

Gültige Subnetzmasken sind:
255.000.000.000 bis 255.255.255.252

Default Gateway/Router:
Die IP-Adresse des Gateways/Router muss im gleichen Subnetz liegen, wie die des Switches.

3.1.2.2 Vergabe von IP-Adressen

Die IP-Adresse ist eine 32 Bit lange Adresse, die aus Netzwerkteil und Benutzerteil besteht. Der Netzwerkteil besteht aus der Netzklasse und der Netzadresse.
Zur Zeit sind fünf Netzklassen definiert, von denen die Klassen A, B und C für heutige Anwendungen genutzt werden. Die Klassen D und E werden sehr selten genutzt. Daher ist es im Regelfall ausreichend, wenn ein Netzteilnehmer nur die Klassen A, B und C „kennt“.

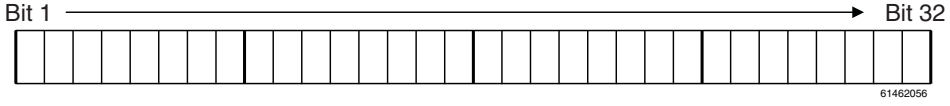


Bild 3-1 Lage der Bits innerhalb der IP-Adresse

Die Netzklasse wird, bei binärer Darstellung der IP-Adresse, durch die ersten Bits dargestellt. Dabei ist die Anzahl der „Einsen“ bis zur ersten „Null“ entscheidend. In der nachfolgenden Tabelle ist die Zuordnung der Klassen dargestellt. Die freien Zellen der Tabelle sind für die Netzklasse nicht mehr relevant und gehören schon zur Netzadresse.

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Klasse A	0				
Klasse B	1	0			
Klasse C	1	1	0		
Klasse D	1	1	1	0	
Klasse E	1	1	1	1	0

Im Anschluss an die Bits der Netzklasse folgen die Bits der Netzwerkadresse und der Benutzeradresse. Je nach Netzklasse stehen sowohl für die Netzadresse (Netz-ID), als auch für die Benutzeradresse (Host-ID) unterschiedlich viele Bits zur Verfügung.

	Netz-ID	Host-ID
Klasse A	7 Bit	24 Bit
Klasse B	14 Bit	16 Bit
Klasse C	21 Bit	8 Bit
Klasse D	28 Bit Multicast-Identifikator	
Klasse E	27 Bit (reserviert)	

Die Darstellung von IP-Adressen kann dezimal oder hexadezimal erfolgen. Um eine logische Zusammengehörigkeit der einzelnen Oktette darzustellen, werden die Oktette, bei dezimaler Darstellung, durch Punkte getrennt (Dotted Decimal Notation).

Durch die Punkte wird die Adresse nicht in Netzwerk- und Benutzeradresse getrennt. Nur die Wertigkeit der ersten Bits (bis zur ersten „Null“) gibt Auskunft über Netzklasse und damit über die Anzahl der verbleibenden Bits der Adresse.

Mögliche Adresskombinationen

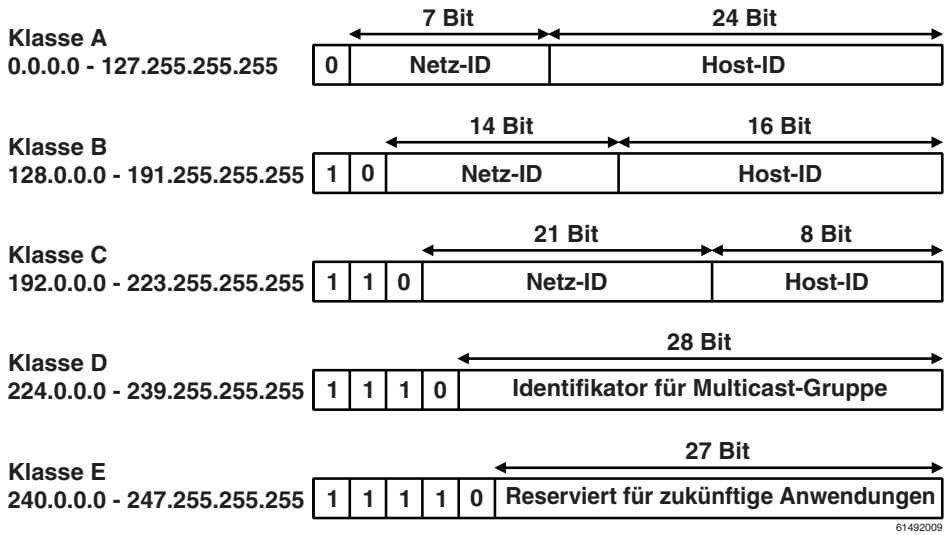


Bild 3-2 Aufbau der IP-Adressen

3.1.2.3 IP-Sonderadressen für spezielle Anwendungen

Einige IP-Adressen sind reserviert, um Sonderfunktionen zu ermöglichen. Die nachfolgend aufgeführten Adressen sollten nicht als Standard-IP-Adressen vergeben werden.

127.x.x.x-Adressen

Die Klasse-A-Netzadresse „127“ ist bei allen Rechnern, unabhängig von der Netzklasse, für eine sogenannte Loopback-Funktion reserviert. Diese Loopback-Funktion darf ausschließlich zu internen Testzwecken der vernetzten Rechner genutzt werden.

Wird ein Telegramm mit dem Wert 127 im ersten Oktett an einen Rechner adressiert, so schickt der Empfänger das Telegramm umgehend an den Sender zurück.

Auf diese Weise kann geprüft werden, ob z. B. die TCP/IP-Software korrekt installiert und konfiguriert ist.

Da die Schichten 1 und 2 des ISO/OSI-Modells nicht in den Test einbezogen sind, sollte zur vollständigen Prüfung die Ping-Funktion verwendet werden.

Wert 255 im Oktett

Der Wert 255 ist als Broadcast-Adresse definiert. Dabei wird das Telegramm an alle Rechner gesendet, die sich im gleichen Netzwerkteil befinden. Beispiele: 004.255.255.255, 198.2.7.255 oder 255.255.255.255 (alle Rechner in allen Netzen). Falls das Netzwerk in Subnetze unterteilt ist, müssen die Subnetz-Masken bei der Berechnung berücksichtigt werden, anderenfalls werden nicht alle Teilnehmer erreicht. Vereinfacht kann gesagt werden, dass die letzte Adresse eines Bereiches als Broadcast-Adresse reserviert ist.

0.x.x.x-Adressen

Der Wert 0 ist als Kennung des eigenen Netzes vergeben. Enthält die IP-Adresse am Anfang eine Null, dann befindet sich der Empfänger im eigenen Netz. Beispiel: 0.2.1.1, gemeint ist der Teilnehmer 2.1.1 in diesem Netz.

Nach einer älteren Definition ist die Null als Broadcast-Adresse vorgesehen. Falls Sie ältere Geräte betreiben, kann es bei Benutzung der IP-Adresse 0.x.x.x zu ungewollten Broadcast und damit zu einer totalen Überlastung des Netzes (Broadcaststorm) kommen.

3.1.2.4 Subnetzmasken

Router und Gateways unterteilen große Netze in mehrere Subnetze. Durch die Subnetzmaske werden die IP-Adressen der einzelnen Geräte bestimmten Subnetzen zugeordnet. Der **Netzwerkteil** einer IP-Adresse wird durch die Subnetzmaske **nicht** verändert. Aus der Benutzeradresse und der Subnetzmaske wird eine erweiterte IP-Adresse generiert. Da das maskierte Subnetz nur den lokalen Rechnern bekannt ist, erscheint allen anderen Teilnehmern diese erweiterte IP-Adresse wie eine Standard-IP-Adresse.

Aufbau der Netzmaske

Die Netzmaske enthält grundsätzlich die gleiche Anzahl an Bits wie eine IP-Adresse. Dabei wird bei der Netzmaske die gleiche Anzahl der Bits (an der gleichen Position) auf „Eins“ gesetzt, die bei der IP-Adresse die Netzklasse widerspiegeln.

Beispiel: Eine IP-Adresse der Klasse A enthält ein Byte Netzadresse und drei Bytes Rechneradresse. Dem entsprechend darf das erste Byte der Subnetzmaske nur „Einsen“ enthalten.

Die verbleibenden Bits (drei Byte) enthalten dann die Adresse des Subnetzes und des Rechners. Durch eine UND-Verknüpfung der Bits der IP-Adresse und der Bits der Subnetz-Maske entsteht dann die erweiterte IP-Adresse. Da das Subnetz nur den lokalen Teilnehmern bekannt ist, erscheint eine solche IP-Adresse allen anderen Teilnehmern wie eine „normale“ IP-Adresse.

Anwendung

Ergibt die UND-Verknüpfung der Adress-Bits die eigene, lokale Netzadresse und die lokale Subnetzadresse, so befindet sich der Teilnehmer im lokalen Netz. Erbringt die UND-Verknüpfung ein anderes Resultat, wird das Datentelegramm an den Subnetz-Router gesendet.

Beispiel für eine Subnetzmaske der Klasse B:

Dezimale Darstellung: 255.255.192.0
Binäre Darstellung: 1111 1111.1111 1111.1100 0000.0000 0000

Durch diese Subnetzmaske unterscheidet die TCP/IP-Protokollsoftware zwischen den Geräten, die an das lokale Subnetz angeschlossen sind und den Geräten, die sich in anderen Subnetzen befinden.

Beispiel: Teilnehmer 1 mit der oben dargestellten Subnetzmaske möchte eine Verbindung mit Teilnehmer 2 aufbauen. Teilnehmer 2 hat die IP-Adresse 59.EA.55.32.

Darstellung der IP-Adresse von Teilnehmer 2:

Hexadezimale Darstellung: 59.EA.55.32
Binäre Darstellung: 0101 1001.1110 1010.0101 0101.0011 0010
61462011

Um festzustellen, ob der Teilnehmer 2 sich im lokalen Subnetz befindet, führt die Software jetzt eine bitweise UND-Verknüpfung der eigenen Subnetzmaske und der IP-Adresse von Teilnehmer 2 durch.

UND-Verknüpfung von Subnetzmaske und IP-Adresse von Teilnehmer 2:

Subnetzmaske:		1111 1111.1111 1111.1100 0000.0000 0000
	UND	
IP-Adresse:		0101 1001.1110 1010.0101 0101.0011 0010
Verknüpfungsergebnis:		0101 1001.1110 1010.0100 0000.0000 0000

61462012

Subnetz

Nach der UND-Verknüpfung stellt die Software fest, dass das gesuchte Subnetz (01) nicht dem lokalen Subnetz (11) entspricht und leitet somit das Datentelegramm an einen Subnetz-Router weiter.

3.1.3 Ablaufdiagramm nach Neustart

3.1.3.1 Laden der Konfigurationsdaten

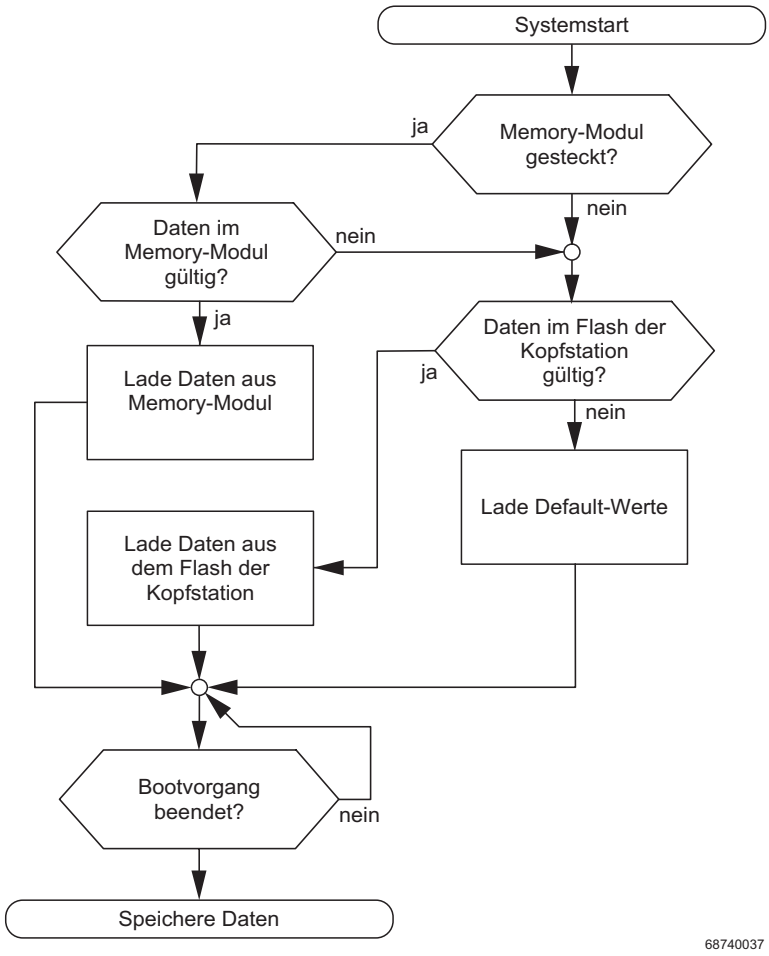


Bild 3-3 Ablaufdiagramm: Laden der Konfigurationsdaten

3.1.3.2 Vergabe der IP-Parameter

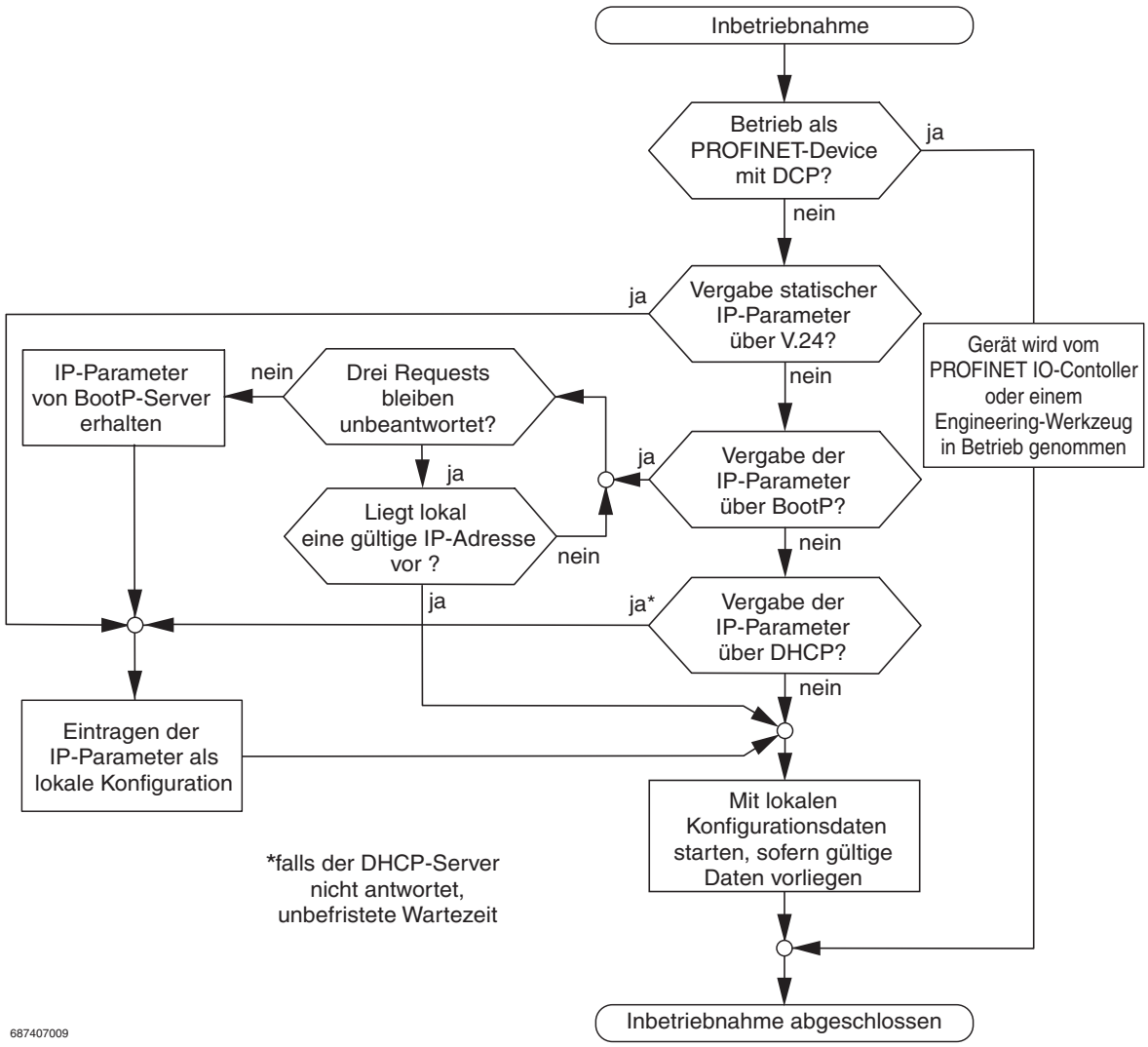


Bild 3-4 Ablaufdiagramm: Vergabe der IP-Parameter

Wenn DHCP als Vergabemechanismus ausgewählt wird, muss der DHCP-Server eine DHCP-Lease-Time von **mindestens fünf** Minuten anbieten, damit der Switch die zugewiesenen IP-Parameter akzeptiert.

3.2 Inbetriebnahme der Interface-Module

Für einen nach GL zertifizierten Betrieb sind nur die in der nachfolgenden Tabelle aufgeführten Interface-Module zulässig.

Tabelle 3-1 Interface-Module mit GL-Zulassung

Bezeichnung	Artikel-Nummer
FL IF MEM 2TX-D	2832483
FL IF 2FX SC-D	2832425
FL IF 2FX SM SC-D	2832205
FL IF 2TX VS-RJ-F	2832344
FL IF 2TX VS-RJ-D	2832357

3.2.1 FL IF 2TX VS-RJ ...

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

3.2.1.1 Auslieferungszustand

Nach dem Stecken der Interface-Module ist die Autonegotiation- und die Autocrossing-Funktion aktiviert. Die Link-Überwachung für die Twisted-Pair-Ports ist nicht aktiviert.

Wird ein Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration weiterhin aktiv.

3.2.1.2 Funktionen

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s oder 100 MBit/s und Übertragungsmodus halb- oder vollduplex) seiner RJ45-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.
– Autocrossing
  Eine Unterscheidung zwischen 1:1- und Cross-Over-Leitungen ist nicht erforderlich, da eine automatische Kreuzung der Sende- und Empfangsleitungen erfolgt.

Autocrossing steht nur dann zur Verfügung, wenn Autonegotiation aktiviert ist.

– Autopolarity
  Ist das Empfangsleiterpaar einer Twisted-Pair-Leitung vertauscht angeschlossen (RD+ und RD- gegeneinander vertauscht), erfolgt durch den Switch automatisch eine Umkehrung der Polarität.

– Leitungsüberwachung
  Mit regelmäßigen Link-Test-Pulsen gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen TP/TX-Leitungssegmente auf Kurzschluss oder Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine TP/TX-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

3.2.1.3 Anschluss der RJ45-Stecker

Stecken Sie den RJ45-Stecker unter der Beachtung der Codierung in die Buchse bis er einrastet. Zum Entfernen des Steckers drücken Sie die Rastnase in Richtung des Steckers (A) und ziehen Sie ihn ab.

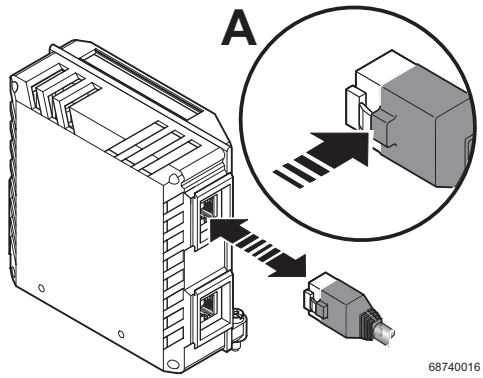


Bild 3-5 Anschluss der RJ45-Stecker

Industrietauglicher RJ45-Stecker mit zusätzlicher Verrastung

Die nachfolgende Abbildung zeigt den VS-08-T-G-RJ45/IP20, der direkt auf das Interface-Modul aufgerastet werden kann.

Bild 3-6 Einsatz des VS-08-T-G-RJ45/IP20

3.2.1.4 Belegung der RJ45-Buchse (TP/TX)

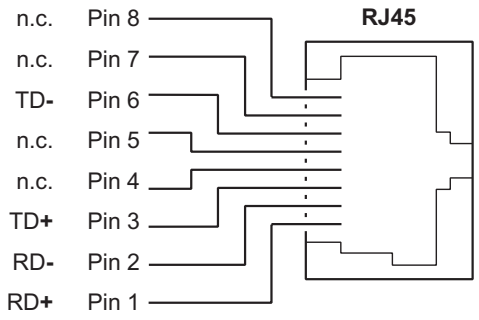


Bild 3-7 Belegung der RJ45-Buchse

3.2.2 FL IF 2POF 10/100 ...

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

3.2.2.1 Auslieferungszustand

Nach dem Stecken der Interface-Module ist die Autonegotiation-Funktion aktiviert, die Link-Überwachung für die POF-Ports ist nicht aktiviert.

Wird ein Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration weiterhin aktiv.

3.2.2.2 Funktionen

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine POF-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s / 100 MBit/s und Übertragungsmodus halb- / vollduplex) seiner F-SMA-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.

3.2.2.3 Anschluss der F-SMA-Stecker

Um Verschmutzungen zu vermeiden, entfernen Sie die Staubschutzkappen erst unmittelbar vor dem Anschluss der Steckverbinder. Gleiches gilt für die Schutzkappen auf den Steckverbindern.

F-SMA ist ein genormter LWL-Anschluss. Wir empfehlen die Verwendung der besonders einfach handhabbaren F-SMA-Stecker mit Schnellspannanschluss von Phoenix Contact. Die Befestigung der Stecker auf dem Interface-Modul erfolgt durch handfestes Anziehen der Überwurfschraube.

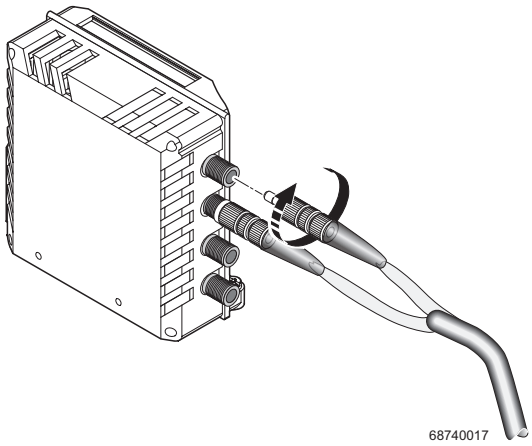


Bild 3-8 Anschluss der F-SMA-Stecker

3.2.2.4 POF-Verbindung zwischen Geräten

Beachten Sie bei der Kopplung von zwei POF-Interface-Modulen die Signalrichtung des Lichtwellenleiters. Der Faseranschluss erfolgt immer von Sender auf Empfänger.

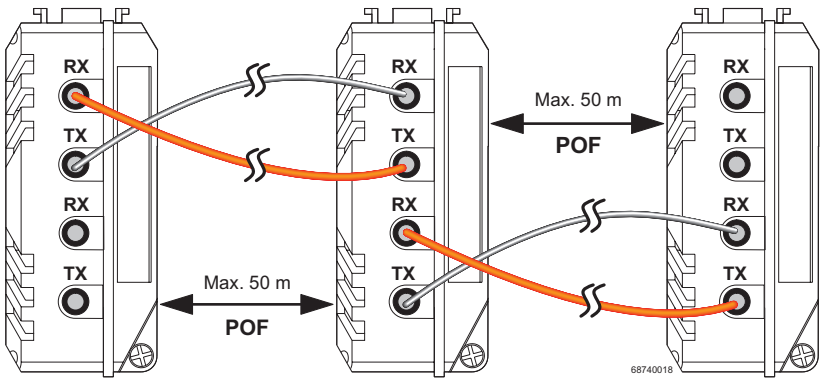


Bild 3-9 POF-Verbindung

3.2.2.5 Absenkung der Sendeleistung

Bei Polymerfaser-LWL-Strecken (POF) < 20 m muss die Sendeleistung abgesenkt werden. Schieben Sie dazu den Schalter auf der Oberseite des Interface-Moduls in die Stellung „OFF“. Achten Sie auf die Zuordnung der Port-Nummer.

Sie können die Schalterstellung im WBM oder per SNMP auslesen.

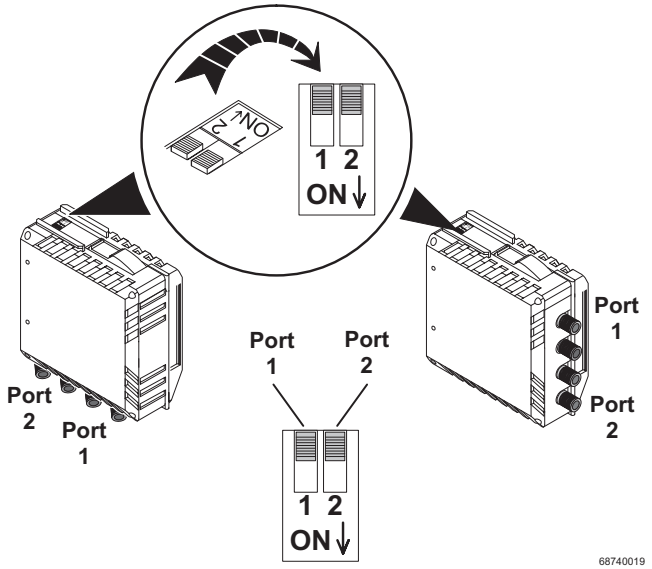


Bild 3-10 Zuordnung der F-SMA-Ports zum DIP-Schalter

3.2.3 FL IF 2HCS 100 ...

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

3.2.3.1 Auslieferungszustand

Nach dem Stecken der Interface-Module ist die Link-Überwachung für die HCS-Ports ist nicht aktiviert.

Ein HCS-Port ist fest auf 100 MBit/s - vollduplex eingestellt. Wird ein HCS-Port entfernt, wird der Port-Modus auf Autonegotiation gestellt.

3.2.3.2 Funktionen

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine HCS-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

3.2.3.3 Anschluss der F-SMA-Stecker

Um Verschmutzungen zu vermeiden, entfernen Sie die Staubschutzkappen erst unmittelbar vor den Anschluss der Steckverbinder. Gleiches gilt für die Schutzkappen auf den Steckverbindern.

F-SMA ist ein genormter LWL-Anschluss. Wir empfehlen die Verwendung der besonders einfach handhabbaren F-SMA-Stecker mit Schnellspannanschluss von Phoenix Contact. Die Befestigung der Stecker auf dem Interface-Modul erfolgt durch handfestes Anziehen der Überwurfschraube.

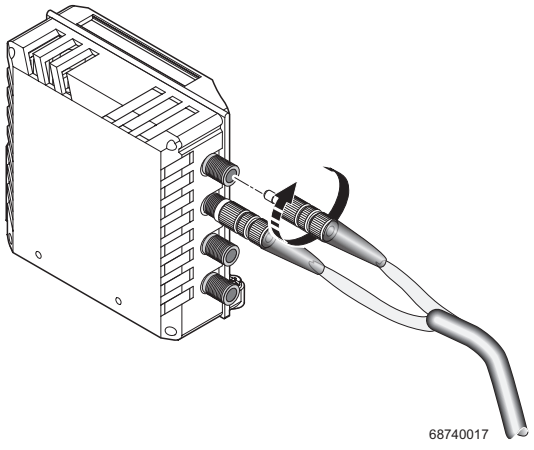


Bild 3-11 Anschluss der F-SMA-Stecker

3.2.3.4 HCS-Verbindung zwischen Geräten

Beachten Sie bei der Kopplung von zwei HCS-Interface-Modulen die Signalrichtung des Lichtwellenleiters. Der Faseranschluss erfolgt immer von Sender auf Empfänger.

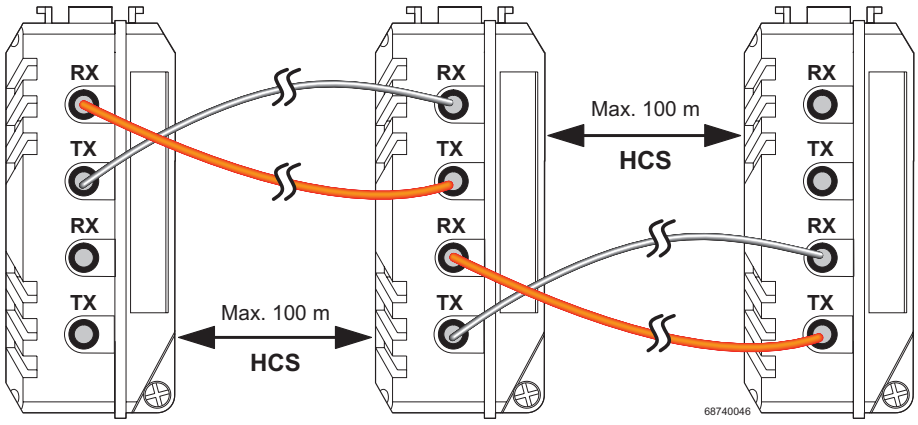


Bild 3-12 HCS-Verbindung

3.2.4 FL IF 2FX SC ... / FL IF 2FX SM SC ...

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

Wird das FL IF 2FX (SM) SC...-Interface entfernt und ein anderer Interface-Typ an dessen Platz gesteckt, werden die Ports auf Autonegotiation umgestellt.

3.2.4.1 Auslieferungszustand

Nach dem Stecken der Interface-Module ist eine Datenübertragungsrate von 100 MBit/s und Vollduplex-Betrieb voreingestellt, die Link-Überwachung für die Lichtwellenleiter-Ports ist nicht aktiviert.

Wird ein Lichtwellenleiter-Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration mit folgenden Ausnahmen weiterhin aktiv:

– Die Datenübertragungsrate wird auf 100 MBit/s und
– das Duplex-Verfahren wird auf vollduplex eingestellt.

Wird das Modul entfernt, wird auf Autonegotiation umgestellt.

3.2.4.2 Funktionen

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine Lichtwellenleiter-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

– Far-End-Fault-Detection zeigt an, dass die Verbindung in Richtung der Gegenstelle nicht in Ordnung ist (die Gegenstelle zeigt keinen Link an) und somit mindestens eine Faser in der Lichtwellenleitung defekt ist oder nicht richtig konfektioniert wurde.

3.2.4.3 Anschluss der SC-D-Stecker

Um Verschmutzungen zu vermeiden, entfernen Sie die Staubschutzkappen erst unmittelbar vor den Anschluss der Steckverbinder. Gleiches gilt für die Schutzkappen auf den Steckverbindern.

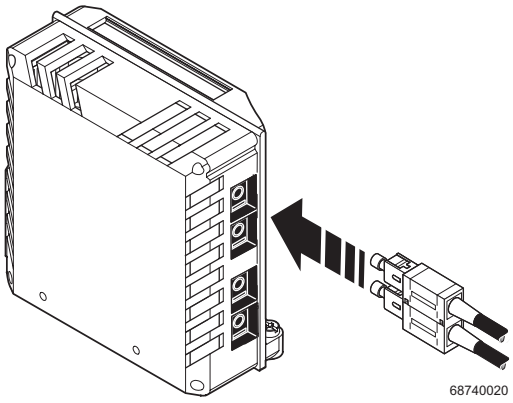


Bild 3-13 Anschluss der SC-D-Stecker

3.2.4.4 Lichtwellenleiter-Verbindung zwischen Geräten

Beachten Sie bei der Kopplung von zwei Lichtwellenleiter-Interface-Modulen die Signalrichtung des Lichtwellenleiters. Der Faseranschluss erfolgt immer von Sender auf Empfänger. Die mit einer Halterung gekoppelten SC-D/SCRJ-Stecker sind so kodiert, dass die Zuordnung von Sende- und Empfangsrichtung passend ist.

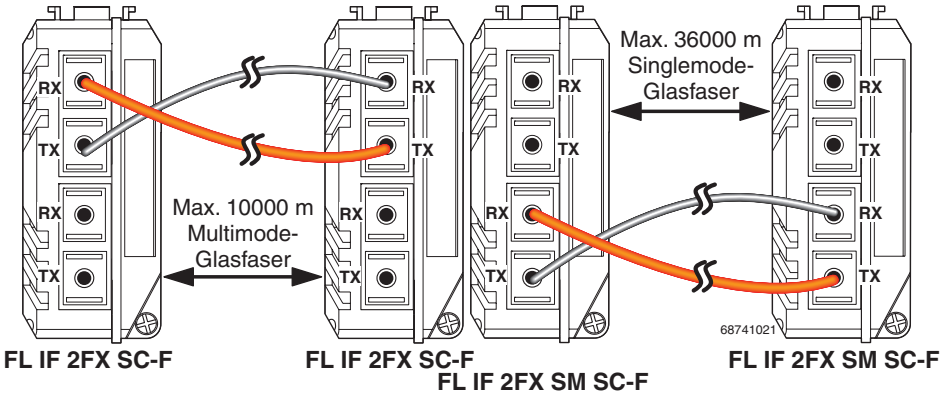


Bild 3-14 Lichtwellenleiter-Verbindung zwischen Geräten

Die maximale Länge der Lichtwellenlweiter ist vom verwendeten Interface-Modul/Fasertyp abhängig.

3.2.5 FL IF 2FX ST-D

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

Wird das FL IF 2FX ST-D-Interface entfernt und ein anderer Interface-Typ an dessen Platz gesteckt, werden die Ports auf Autonegotiation umgestellt.

3.2.5.1 Auslieferungszustand

Nach dem Stecken der Interface-Module ist eine Datenübertragungsrate von 100 MBit/s und Vollduplex-Betrieb voreingestellt, die Link-Überwachung für die Glasfaser-Ports ist nicht aktiviert.

Wird ein Glasfaser-Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration mit folgenden Ausnahmen weiterhin aktiv:

– Die Datenübertragungsrate wird auf 100 MBit/s und
– das Duplex-Verfahren wird auf vollduplex eingestellt.

Wird das Modul entfernt, wird auf Autonegotiation umgestellt.

3.2.5.2 Funktionen

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine Glasfaser-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

– Far-End-Fault-Detection zeigt an, dass die Verbindung in Richtung der Gegenstelle nicht in Ordnung ist (die Gegenstelle zeigt keinen Link an) und somit mindestens eine Faser in der Glasfaserleitung defekt ist oder nicht richtig konfektioniert wurde.

3.2.5.3 Anschluss der ST-Stecker

Um Verschmutzungen zu vermeiden, entfernen Sie die Staubschutzkappen erst unmittelbar vor dem Anschluss der Steckverbinder. Gleiches gilt für die Schutzkappen auf den Steckverbindern.

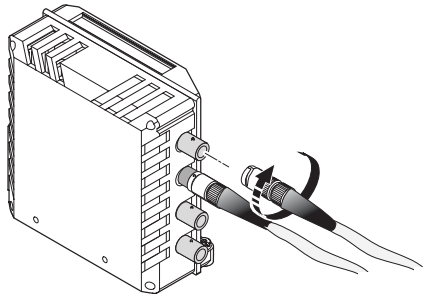


Bild 3-15 Anschluss der ST-Stecker

3.2.5.4 Glasfaser-Verbindung zwischen Geräten

Beachten Sie bei der Kopplung von zwei Glasfaser-Interface-Modulen die Signalrichtung des Lichtwellenleiters. Der Faseranschluss erfolgt immer von Sender auf Empfänger.

Die maximale Länge der Glasfaserleitungen ist vom verwendeten Fasertyp abhängig.

3.2.6 FL IF TX/POF 10/100 ...

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

3.2.6.1 Auslieferungszustand

Nach dem Stecken der Interface-Module sind die Autonegotiation- und die Autocrossing-Funktion bei dem Twisted-Pair-Port aktiviert, beim POF-Port ist die Autonegotiation-Funktion aktiviert. Die Port-Überwachung für beide Ports ist nicht aktiviert.

Wird ein Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration weiterhin aktiv.

3.2.6.2 Funktionen der POF-Schnittstelle

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine POF-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s / 100 MBit/s und Übertragungsmodus halb- / vollduplex) seiner F-SMA-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.

3.2.6.3 Funktionen der Twisted-Pair-Schnittstelle

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s / 100 MBit/s und Übertragungsmodus halb- / vollduplex) seiner RJ45-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.
– Autocrossing
  Eine Unterscheidung zwischen 1:1- und Cross-Over-Leitungen ist nicht erforderlich, da eine automatische Kreuzung der Sende- und Empfangsleitungen erfolgt.

Autocrossing steht nur dann zur Verfügung, wenn Autonegotiation aktiviert ist.

– Autopolarity
  Ist das Empfangsleiterpaar einer Twisted-Pair-Leitung vertauscht angeschlossen (RD+ und RD- gegeneinander vertauscht), erfolgt durch den Switch automatisch eine Umkehrung der Polarität.
– Leitungsüberwachung
  Mit regelmäßigen Link-Test-Pulsen gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen TP/TX-Leitungssegmente auf Kurzschluss oder Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine TP/TX-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

3.2.6.4 Netzwerk-Anschluss

Die Schalterstellung der Sendeleistungsabsenkung wird erst bei zukünftigen Hardware-Versionen im Web-Interface angezeigt.

Siehe „FL IF 2TX VS-RJ ...“ auf Seite 3-9 ff und „FL IF 2POF 10/100 ...“ auf Seite 3-11 ff.

3.2.7 FL IF TX/HCS 100 ...

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

3.2.7.1 Auslieferungszustand

Nach dem Stecken der Interface-Module sind die Autonegotiation- und die Autocrossing-Funktion bei dem Twisted-Pair-Port aktiviert, beim HCS-Port ist die Datenübertragungsrate fest auf 100 MBit/s vollduplex eingestellt. Die Port-Überwachung für beide Ports ist nicht aktiviert.

Wird ein Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration weiterhin aktiv.

3.2.7.2 Funktionen der HCS-Schnittstelle

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine HCS-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

3.2.7.3 Funktionen der Twisted-Pair-Schnittstelle

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s / 100 MBit/s und Übertragungsmodus halb- / vollduplex) seiner RJ45-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.
– Autocrossing
  Eine Unterscheidung zwischen 1:1- und Cross-Over-Leitungen ist nicht erforderlich, da eine automatische Kreuzung der Sende- und Empfangsleitungen erfolgt.

Autocrossing steht nur dann zur Verfügung, wenn Autonegotiation aktiviert ist.

– Autopolarity
  Ist das Empfangsleiterpaar einer Twisted-Pair-Leitung vertauscht angeschlossen (RD+ und RD- gegeneinander vertauscht), erfolgt durch den Switch automatisch eine Umkehrung der Polarität.
– Leitungsüberwachung
  Mit regelmäßigen Link-Test-Pulsen gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen TP/TX-Leitungssegmente auf Kurzschluss oder Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine TP/TX-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

3.2.7.4 Netzwerk-Anschluss

Siehe „FL IF 2TX VS-RJ ...“ auf Seite 3-9 ff und „FL IF 2HCS 100 ...“ auf Seite 3-14 ff.

3.2.8 FL IF MEM 2TX-D / FL IF MEM 2TX-D/MRM

Stellen Sie sicher, dass immer nur ein Memory-Modul gesteckt ist. Falls mehr als ein Modul gesteckt sind, zeigt der Switch den Fehler-Code „87“ im Display an. Bitte entfernen Sie dann alle Memory-Module bis auf eines und starten Sie den Switch erneut.

Das Interface-Modul verfügt neben dem Parametrierungsspeicher über zwei Twisted-Pair-Schnittstellen. Damit es von den anderen 2TX-Interface-Modulen zu unterscheiden ist, wird es in einem anthrazit-farbenem Gehäuse geliefert. Der Parametrierungsspeicher dient zur Ablage von Gerätedaten, die vom Benutzer geändert und nichtflüchtig abgespeichert werden sollen.

Das Memory-Modul wird ab der Firmware-Version 2.03 unterstützt. Bei einer Firmware-Version <2.03 wird das Memory-Modul wie ein „normales“ FL IF 2TX VS-RJ behandelt.

Der Einsatz des Memory-Modules setzt in der Kopfstation die Systembus-Firmware 4.20 oder höher voraus. Auf der Webseite „Device Information/General“ wird die Systembus-Firmware Ihrer Kopfstation angezeigt.

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

Wird das Modul während des Speichervorgangs entfernt, wird die Konfiguration nicht gespeichert. Der Speichervorgang ist beendet, wenn im Display **nicht** mehr „SC“ angezeigt wird oder auf der Webseite **„Configuration Management“** der Status „Current Configuration was saved“ angezeigt wird.

3.2.8.1 Auslieferungszustand des Parametrierungsspeichers

Im Auslieferungszustand ist der Parametrierungsspeicher leer (siehe „Auslieferungszustand / Werkseinstellungen“ auf Seite 3-1).

3.2.8.2 Auslieferungszustand der Twisted-Pair-Schnittstelle

Nach dem Stecken der Interface-Module sind die Autonegotiation- und die Autocrossing-Funktion aktiviert. Die Link-Überwachung für die Twisted-Pair-Ports ist nicht aktiviert.

Wird ein Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration weiterhin aktiv.

3.2.8.3 Funktion des Memory-Moduls

– Beim Speichern der Daten in das Flash des Gerätes werden die Daten auch in ein gestecktes Memory-Modul übertragen.

Wird der Auslieferungszustand durch den Benutzer wiederhergestellt, wird die Konfiguration auch auf das Memory-Modul gespeichert. Siehe „Auslieferungszustand / Werkseinstellungen“ auf Seite 3-1.

– Daten werden im Flash der Kopfstation und im Memory-Modul gespeichert:
  - Nach einem Systemstart oder
  - auf Benutzeranforderung.

– Beim Starten des MMS werden die Daten aus einem gesteckten Memory-Modul gelesen (Display zeigt „OP“) und als aktuelle Konfiguration verwendet. Dabei werden die Daten im Flash mit denen des Memory-Modules überschrieben.

Beachten Sie, dass auch das auf dem Memory-Modul hinterlegte Passwort auf den MMS übertragen wird. Stellen Sie sicher, dass Ihnen das Passwort der Konfiguration auf dem Memory-Modul bekannt ist.

3.2.8.4 Funktionen der Twisted-Pair-Schnittstelle

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s / 100 MBit/s und Übertragungsmodus halb- / vollduplex) seiner RJ45-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.
– Autocrossing
  Eine Unterscheidung zwischen 1:1- und Cross-Over-Leitungen ist nicht erforderlich, da eine automatische Kreuzung der Sende- und Empfangsleitungen erfolgt.

Autocrossing steht nur dann zur Verfügung, wenn Autonegotiation aktiviert ist.

– Autopolarity
  Ist das Empfangsleiterpaar einer Twisted-Pair-Leitung vertauscht angeschlossen (RD+ und RD- gegeneinander vertauscht), erfolgt durch den Switch automatisch eine Umkehrung der Polarität.
– Leitungsüberwachung
  Mit regelmäßigen Link-Test-Pulsen gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen TP/TX-Leitungssegmente auf Kurzschluss oder Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine TP/TX-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

3.2.8.5 Netzwerk-Anschluss

Siehe „FL IF 2TX VS-RJ ...“ auf Seite 3-9 ff.

3.2.9 FL IF 2PSE-F

Das PoE-Interface-Modul wird ab der Firmware-Version 4.0 unterstützt. Bei einer Firmware-Version <4.0 wird das Modul wie ein Standard-RJ45-Interface-Modul behandelt. Ohne Unterstützung durch die Firmware und die Hardware (Systembus) (siehe folgenden Hinweis) kann das Modul im PoE-Modus ohne jedes Management betrieben werden. Es stehen dann keine Konfigurationsmöglichkeiten und keine Diagnosedaten zur Verfügung, angeschlossene Endgeräte werden aber dennoch mit Spannung versorgt.

Der Einsatz des PoE-Interface-Moduls setzt in der Kopfstation die Systembus-Firmware 5.00 oder höher und in den Erweiterungsmodulen die Systembus-Firmware 4.00 oder höher voraus. Ist in der Kopfstation oder in irgendeinem Erweiterungsmodul diese Bedingung nicht erfüllt, so steht das PoE-Management im **gesamten** System nicht zur Verfügung. Auf der Webseite „Device Information/General“ wird die Systembus-Firmware angezeigt.

Das PoE-Management und die PoE-Informationen stehen nur dann zur Verfügung, wenn an das jeweiligen PoE-Interface-Modul die 48-V-Versorgung angeschlossen ist. Ohne angeschlossene Versorgung können die Ports als Standard-RJ45-Ports genutzt werden.

Eigenschaften des PoE-Betriebs

– Es können bis zu zwölf PoE-Interface-Module mit insgesamt 24 Ports gleichzeitig am MMS betrieben werden.
– Die Konfiguration ist ohne gestecktes Interface-Modul und ohne angeschlossene 48-V-Versorgung möglich.
– Das PoE-Management und die PoE-Informationen stehen nur bei gestecktem Interface-Modul und bei angeschlossener 48-V-Versorgung zur Verfügung.
– Folgende Management-Funktionen stehen zur Verfügung:
  - Fehlerzustände je Port auf dem Display anzeigen und über den Alarmkontakt melden (ja/nein)
  - Spannung je Port ein-/ausschalten
  - Strombegrenzung für Verbraucher, die sich als Klasse 1 (Class 1) Geräte klassifiziert haben, ein- oder ausschalten.
– Versenden von Traps bei Änderung des PoE-Status
– Folgende Diagnose-Angaben werden angezeigt:
  - Kein Fehler
  - Überspannung/Unterspannung
  - Thermischer Fehler
  - Überlast
  - Disconnected Load (die Stromaufnahme an diesem Port beträgt weniger als 10 mA, die Versorgungsspannung wird vom PoE-Modul abgeschaltet)
  - 48-V-Versorgung fehlt
  - Kein PoE-Interface-Modul an diesem Port erkannt
  - Fehlende Hardware-Unterstützung aufgrund des Systembusses
  - Die detektierte Klasse eines angeschlossenen Endgerätes (Class 0 bis Class 4)
  - Die Ausgangsspannung sowie den Ausgangsstrom

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

3.2.9.1 Auslieferungszustand

Nach dem Stecken der Interface-Module sind die Autonegotiation- und die Autocrossing-Funktion aktiviert. Die Link-Überwachung für die Twisted-Pair-Ports ist nicht aktiviert.

Wird ein Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration weiterhin aktiv.

3.2.9.2 Funktionen

– Autonegotiation
  Autonegotiation ist ein Verfahren, bei dem der Switch automatisch die Betriebsparameter des angeschlossenen Netzes erkennt und entsprechend die Parameter (Datenübertragungsrate 10 MBit/s oder 100 MBit/s und Übertragungsmodus halb- oder vollduplex) seiner RJ45-Ports einstellt. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über das Web-Interface aktiviert/deaktiviert werden.
– Autocrossing
  Eine Unterscheidung zwischen 1:1- und Cross-Over-Leitungen ist nicht erforderlich, da eine automatische Kreuzung der Sende- und Empfangsleitungen erfolgt.

Autocrossing steht nur dann zur Verfügung, wenn Autonegotiation aktiviert ist.

– Autopolarity
  Ist das Empfangsleiterpaar einer Twisted-Pair-Leitung vertauscht angeschlossen (RD+ und RD- gegeneinander vertauscht), erfolgt durch den Switch automatisch eine Umkehrung der Polarität.
– Leitungsüberwachung
  Mit regelmäßigen Link-Test-Pulsen gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen TP/TX-Leitungssegmente auf Kurzschluss oder Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine TP/TX-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

Die PoE-Konfigurationsmöglichkeiten stehen auch dann zur Verfügung, wenn kein PoE-Interface-Modul gesteckt ist. Wird ein PoE-Interface-Modul gesteckt, so wird die Konfiguration nach einigen Sekunden auf das Modul übertragen.

3.2.9.3 Netzwerk-Anschluss

Siehe „FL IF 2TX VS-RJ ...“ auf Seite 3-9 ff.

3.2.9.4 Anschluss der 48-V-PoE-Versorgungsspannung

Stecken der PoE-Versorgung

Der Stecker der PoE-Versorgung befindet sich an der Unterseite des Interface-Moduls. Beachten Sie beim Stecken die Codierung des Steckers.
Das Modul besitzt je Port eine grüne LED, die den PoE-Betrieb anzeigt. Die LED ist aktiv, wenn die PoE-Versorgung **und** ein PD (Powered Device) angeschlossen ist. Die LED blinkt, wenn das Modul mit weniger als 48 V versorgt wird.

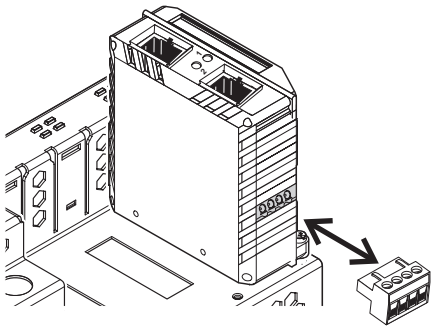


Bild 3-16 Stecken des PoE-Versorgungssteckers

Anschließen der PoE-Versorgung

Schließen Sie die 48-V-PoE-Versorgung an die Klemmen 1 (+) und 2 (-) an. Die Klemmen sind im Modul gebrückt. Die Brücken befinden sich zwischen Klemme 1 und 3 sowie zwischen Klemme 2 und 4. Die Brücken können genutzt werden, um bis zu **maximal** drei weitere PoE-Interface-Module mit Spannung zu versorgen. Bei weiteren PoE-Interface-Modulen muss die Versorgungsspannung erneut vom Netzteil eingespeist werden.

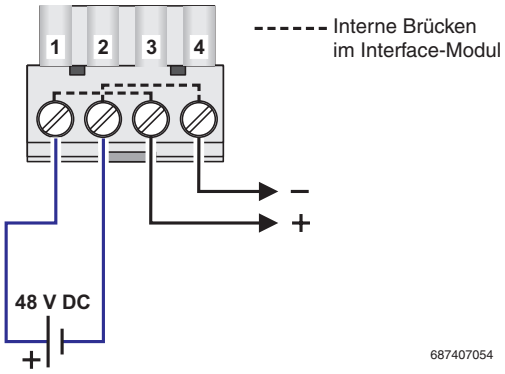


Bild 3-17 Anschluss der 48-V-PoE-Versorgung

Tabelle 3-2 Pinbelegung der PoE-Ports

Pin	Belegung	Beschreibung	Pin	Belegung	Beschreibung
1	RX+ / 48 V DC	Daten/PoE +	5	n. c.	-
2	RX- / 48 V DC	Daten/PoE +	6	TX- / 0 V	Daten/PoE-
3	TX+ / 0 V	Daten/PoE -	7	n. c.	-
4	n. c.	-	8	n. c.	-

3.2.10 FL IF 2POF SCRJ-D

Hot-Plugging
Beim Stecken oder Ziehen der Interface-Module ist das Abschalten der Versorgungsspannung **nicht** notwendig. Die Interface-Module werden automatisch erkannt und beim Netzwerk-Management angemeldet.

Wird das FL IF 2POF SCRJ ...-Interface entfernt und ein anderer Interface-Typ an dessen Platz gesteckt, werden die Ports auf Autonegotiation umgestellt.

3.2.10.1 Auslieferungszustand

Nach dem Stecken der Interface-Module ist eine Datenübertragungsrate von 100 MBit/s und Vollduplex-Betrieb voreingestellt, die Link-Überwachung für die Lichtwellenleiter-Ports ist nicht aktiviert.

Wird ein Lichtwellenleiter-Interface-Modul auf einen bereits parametrierten MMS gesteckt, bleibt die vorhandene Konfiguration mit folgenden Ausnahmen weiterhin aktiv:

– Die Datenübertragungsrate wird auf 100 MBit/s und
– das Duplex-Verfahren wird auf vollduplex eingestellt.

Wird das Modul entfernt, wird auf Autonegotiation umgestellt.

3.2.10.2 Funktionen

– Leitungsüberwachung
  Gemäß der Norm IEEE 802.3 überwacht der Switch die angeschlossenen LWL-Leitungen auf Unterbrechung.

Ein nicht belegter Port wird als Leitungsunterbrechung gewertet. Ebenso wird eine Lichtwellenleiter-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung gewertet, da das angeschlossene, aber stromlose Gerät keine Link-Test-Pulse senden kann.

– Far-End-Fault-Detection zeigt an, dass die Verbindung in Richtung der Gegenstelle nicht in Ordnung ist (die Gegenstelle zeigt keinen Link an) und somit mindestens eine Faser in der Lichtwellenleitung defekt ist oder nicht richtig konfektioniert wurde.

3.2.10.3 Anschluss der SCRJ-Stecker

Um Verschmutzungen zu vermeiden, entfernen Sie die Staubschutzkappen erst unmittelbar vor den Anschluss der Steckverbinder. Gleiches gilt für die Schutzkappen auf den Steckverbindern.

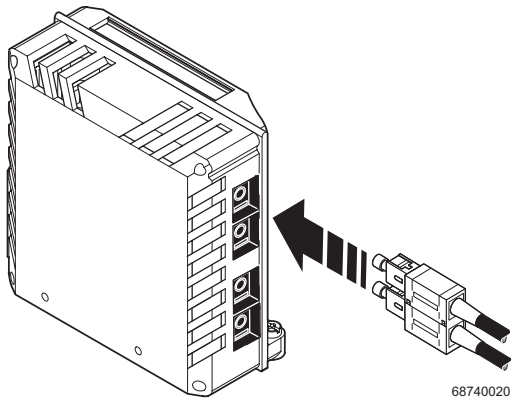


Bild 3-18 Anschluss der SCRJ-Stecker

3.2.10.4 Lichtwellenleiter-Verbindung zwischen Geräten

Beachten Sie bei der Kopplung von zwei Lichtwellenleiter-Interface-Modulen die Signalrichtung des Lichtwellenleiters. Der Faseranschluss erfolgt immer von Sender auf Empfänger. Die mit einer Halterung gekoppelten SCRJ-Stecker sind so kodiert, dass die Zuordnung von Sende- und Empfangsrichtung passend ist.

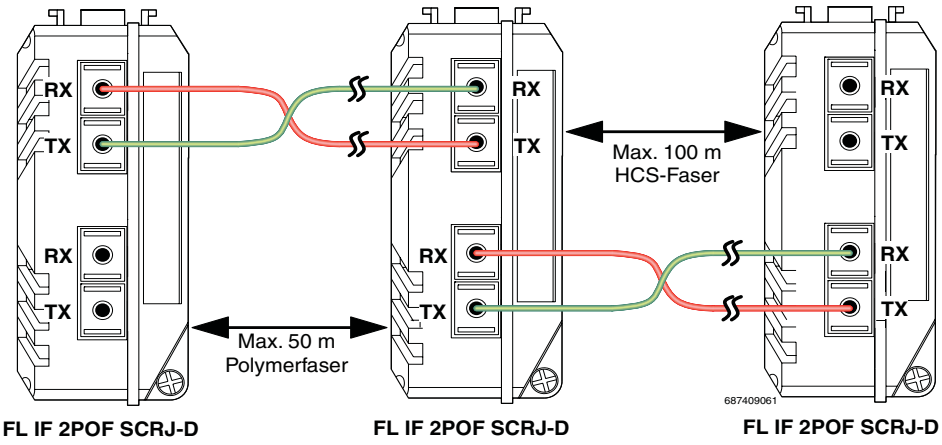


Bild 3-19 Lichtwellenleiter-Verbindung zwischen Geräten

Die maximale Länge der Lichtwellenlweiter ist vom verwendeten Interface-Modul/Fasertyp abhängig.

3.2.10.5 SCRJ-Module im WBM

Informationen über die SCRJ-Module werden sehr detailliert im WBM (siehe Kapitel „Menü „Ports\Port POF Table““ auf Seite 4-30) dargestellt, anzeigt werden z. B. die Port-System-Reserve, Alarme oder Port-Stati.

Die folgenden Stati können unter „Transceiver status“ angezeigt werden:

– System Hardware does not support diagnoseable POF modules“ (Diese Hardware unterstützt keine POF-SCRJ-Diagnose)
– No POF-SCRJ Interface modules present (Es ist kein POF-SCRJ-Modul gesteckt)
– POF-SCRJ Interface module is present and OK (Die Systemreserve ist größer 2 dB und wird unter „RX system reserve angezeigt)
– POF-SCRJ Interface module is present, but the system reserve is low (Die Systemreserve ist kleiner 2 dB, aber größer 0 dB)
– POF-SCRJ Interface module is present, but the system reserve is exhausted (Keine Systemreserve vorhanden - die empfangene Lichtleistung liegt unterhalb des erforderlichen Mindestwertes)

3.3 Frame-Switching

Der FL SWITCH MM HS arbeitet im Store-and-Forward-Modus. Während des Empfangs eines Datenpakets analysiert der Switch die Quell- und Zieladressen. In seiner Adresstabelle speichert der Switch bis zu 8000 MAC-Adressen mit einer einstellbaren Aging Time von 10 bis 825 Sekunden.

3.3.1 Store and Forward

Alle Datentelegramme, die der Switch empfängt, werden gespeichert und auf ihre Gültigkeit geprüft. Ungültige oder fehlerhafte Datenpakete (>1522 Byte oder CRC-Fehler) sowie Fragmente (<64 Byte) werden verworfen. Gültige Datentelegramme werden vom Switch weitergeleitet.

3.3.2 Multiaddress-Fähigkeit

Der Switch lernt alle Quelladressen je Port. Nur Pakete mit

– unbekannten Quelladressen,
– einer Quelladresse dieses Ports oder
– einer Multi-/Broadcast-Adresse

im Zieladressfeld werden über den betreffenden Port weitergeleitet. Der Switch kann bis zu 8000 Adressen lernen. Dies wird notwendig, wenn an einem oder an mehreren Ports mehr als ein Endgerät angeschlossen ist. Es können mehrere eigenständige Subnetze an einen Switch angeschlossen werden.

3.3.3 Adressen lernen

Der MMS erlernt selbstständig durch Auswertung der Quelladressen in den Datentelegrammen die Adressen der Endgeräte, die über diesen Port angeschlossen sind. Empfängt der MMS ein Datentelegramm, dann leitet er dieses nur an den Port weiter, über den der gewünschte Teilnehmer zu erreichen ist (wenn die Adresse zuvor gelernt werden konnte).
Der MMS kann bis zu 8000 Adressen lernen und in seiner Tabelle speichern. Der Switch überwacht das Alter der gelernten Adressen. Adresseinträge, die ein bestimmtes Alter (Default: 40 Sekunden, einstellbar von 10 bis 825 Sekunden, Aging Time) überschreiten, löscht der Switch selbstständig aus seiner Adresstabelle.

Ein Neustart löscht alle gelernten Adresseinträge.

Eine Auflistung der erkannten MAC-Adressen finden Sie in der MAC-Address-Tabelle (siehe Kapitel „Menü „Diagnostics\Mac Address Table““ auf Seite 4-40). Die MAC-Adress-Tabelle kann über den „Clear“-Button gelöscht werden.

Die Aging-Time wird über das MIB-Objekt „dot1dTpAgingTime“ (OID 1.3.6.1.2.1.17.4.2) eingestellt. Der mögliche Einstellbereich beträgt 10 - 825 Sekunden. Bei statischer Konfiguration wird eine Aging-Time von 300 Sekunden empfohlen.

3.3.4 Priorisierung

Der Switch unterstützt zur Beeinflussung der internen Paketabarbeitungsreihenfolge zwei Priority Queues (Traffic Classes nach IEEE 802.1D). Die Zuordnung von empfangenen Datentelegrammen zu diesen Klassen erfolgt entweder durch die im VLAN-/Prioritätstag enthaltene Priorität des Datenpaketes, wobei

– Datenpakete mit dem Wert „0“ bis „3“ im Prioritätsfeld mit niedriger (Default) Priorität vermittelt werden und
– Datenpakete mit dem Wert „4“ bis „7“ im Prioritätsfeld mit hoher Priorität durch den Switch vermittelt werden.

Außerdem kann an dem Switch eine Port-basierende Gewichtung von Datenströmen vorgenommen werden.

3.3.4.1 VLAN-/Prioritätstag

Der MMS verarbeitet eingehende Datenpakete unter Beachtung der im Ethernet-Paket enthaltenen Prioritätsinformation (VLAN-/Prioritätstag).

Im Tag ist die Angabe einer Prioritätsstufe von 0 bis 7 möglich, die der MMS in seine beiden internen Warteschlangen einordnet. Im Auslieferungszustand werden die Pakete mit den Prioritäten 0 bis 3 als niederpriore Pakete behandelt und die Pakete mit Prio 4 bis 7 als hochpriore Ethernet-Pakete.

Die Zuordnung der Prioritätsstufen zu den beiden internen Prioritätsebenen des MMS kann über die „dot1dTrafficClassTable“ der P-Bridge-MIB geändert werden.

Bearbeitungsregeln

Der Switch-Controller im MMS leitet empfangene Pakete nach folgenden Entscheidungen in die beiden Empfangs-Queue:

– BPDU-Pakete (Spanning Tree, LLDP) und IGMP-Pakete werden immer in die hochpriore Queue eingeordnet.
– Pakete mit unbekannten Unicast-Adressen werden immer in die niederpriore Queue eingeordnet.
– Pakete werden in die hochpriore Queue eingeordnet, wenn die Priorität aus dem VLAN-/Prioritäts-Tag auf die Ebene „High“ abgebildet wird (Default Priorität 4 bis 7).
– Die interne Port-Priorität „High“ führt zur Behandlung mit Prioritätsstufe 7, das heißt, dass in den Grundeinstellungen zur Einordnung der Datenpakete in die hochpriore Queue erfolgt.
– Alle verbleibenden Daten werden in die niederpriore Queue eingeordnet.

3.3.4.2 Port-Priorisierung

Zusätzlich zu der Bearbeitungsreihenfolge anhand der Prioritätsinformation aus dem Tag kann der Anwender am MMS eine interne Priorisierung/Bevorzugung pro Switch-Port vorgeben. Damit kann erreicht werden, dass Ethernet-Daten eines Ports bevorzugt bearbeitet werden.

Das Verfahren der Port-Priorisierung ist für Endgeräte geeignet, die kein Tagging unterstützen und somit keine Prioritäten generieren können.

Eine Port-Priorisierung „High“ setzt die interne Priorität der an diesem Port empfangenen Pakete auf die Prioritätsstufe 7. Diese Pakete werden also im Switch behandelt wie Pakete mit Prioritätsinformation 7 im Tag (die bevorzugte Behandlung und Weiterleitung erfolgt nur innerhalb des MMS bevorzugt, beim Weiterleiten an den Empfänger sind die Pakete wieder im Original-Zustand). Die Port-Priorisierung „Low“ hat zur Folge, dass die Priorisierung der an diesem Port empfangenen Pakete durch den Switch nicht beeinflusst werden. Das bedeutet, dass evtl. vorhandene Tags berücksichtig werden oder sonstige Prioritätsregeln angewendet werden.

Einstellung der Port-Priorität

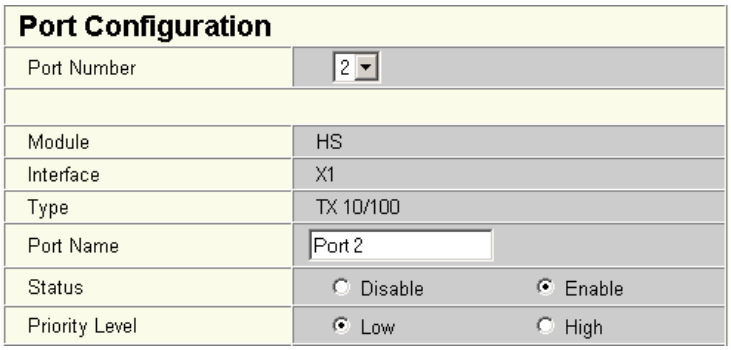


Bild 3-20 Einstellung der Port-Priorität

– Auf der Webseite „Port Configuration“ können Sie unter „Priority Level“ die beiden möglichen Prioritätsstufen wählen.

3.3.4.3 Strict Priority

Der Switch unterstützt zur Beeinflussung der Paketbearbeitungsreihenfolge zwei Priority Queues (Traffic Classes nach IEEE 802.1D). Die Zuordnung von empfangenen Datentelegrammen zu diesen Klassen erfolgt entweder durch die im VLAN-/Prioritäts-Tag enthaltene Priorität des Datenpaketes, wobei

– Datenpakete mit dem Wert „0“ bis „3“ im Prioritätsfeld mit niedriger Priorität vermittelt werden (Default) und
– Datenpakete mit dem Wert „4“ bis „7“ im Prioritätsfeld mit hoher Priorität durch den Switch vermittelt werden.

Der MMS verwendet „Strict Priority“ für die Vermittlung der Datentelegramme. Dabei werden zuerst **alle** Datenpakete mit hoher Priorität vermittelt, erst wenn diese weitergeleitet sind, werden niederpriore Telegramme vermittelt.

Mit dieser Funktion wird verhindert, dass Datenverkehr höherer Priorität in Zeiten starker Verkehrslast durch den niederprioren Datenverkehr gestört wird. Der niederpriore Verkehr wird verworfen, wenn der Speicher oder der Datenkanal überlastet ist.

4 Konfiguration und Diagnose

Das Modular Managed Switch System bietet mehrere User-Interfaces für den Zugriff auf Konfigurations- und Diagnose-Daten. Bevorzugte Schnittstellen sind das Web-Interface und das SNMP-Interface. Über diese beiden Interfaces können jeweils alle Einstellungen vorgenommen und alle Informationen abgefragt werden.
Der Zugriff über Telnet/V.24-Schnittstelle gestattet lediglich den Zugriff auf Basisinformationen. Über die V.24-Schnittstelle kann zusätzlich bei defekter Firmware ein Firmware-Update über XMODEM durchgeführt werden.

Vorgenommene Einstellungen werden nicht automatisch dauerhaft gespeichert. Eine dauerhafte Speicherung der jetzigen Konfiguration erreichen Sie mit „Save current configuration“ auf der Webseite „Configuration Management“.

4.1 Factory Manager

4.1.1 Allgemeine Funktion

Durch die Integration des MMS in den Factory Manager werden Konfiguration und Management optimal unterstützt.

4.1.2 Vergabe der IP-Parameter

Hier ist beispielhaft **eine** Möglichkeit zur Vergabe der IP-Parameter mit dem Factory Manager 2.2 beschrieben.

Nachdem Sie alle erforderlichen Verbindungen hergestellt und den Factory Manager gestartet haben, sollten Sie jetzt den MMS starten oder einen Reset auslösen.

Nach der Bootphase sendet der MMS jetzt die BootP-Requests ab, die vom Factory Manager empfangen und im Meldungsfenster angezeigt werden. Falls Sie andere Teilnehmer im gleichen Netz betreiben, ist es möglich, dass auch Meldungen anderer Teilnehmer angezeigt werden. Sie können die Meldungen von Factory-Line-Komponenten von Phoenix-Contact an der MAC-Adresse erkennen. Sie beginnt mit 00.A0.45 ... und ist auch auf den Geräten angebracht.

Bitte überprüfen Sie die MAC-Adresse in den Meldungen, um das richtige Gerät zu adressieren.

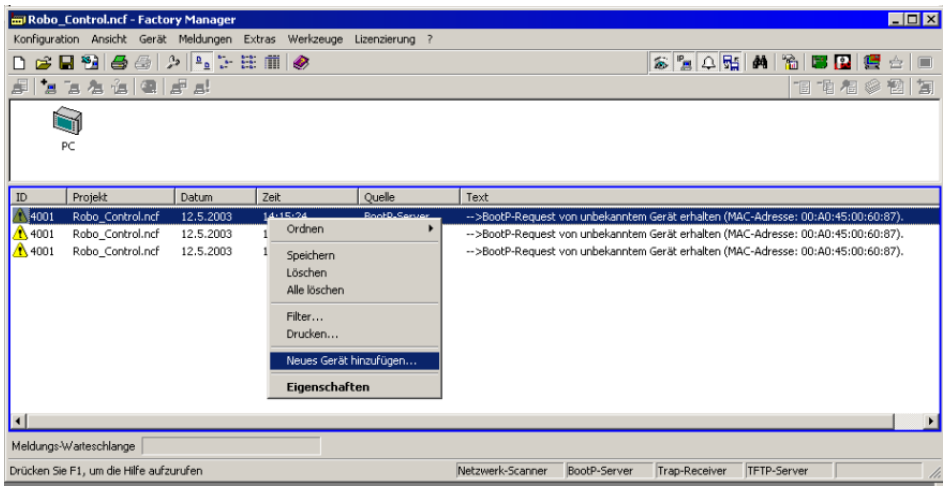


Bild 4-1 Meldungen vom MMS im Factory Manager

Klicken Sie jetzt mit der rechten Maustaste auf eine der Meldungen des MMS und wählen Sie das Menü „Neues Gerät hinzufügen ...“. Unter „Beschreibung“ wählen Sie ein Icon aus und vergeben einen Gerätenamen.

Unter „TCP/IP“ vergeben Sie die gewünschten IP-Parameter (siehe auch Kapitel „Vergabe der IP-Parameter“ auf Seite 3-2).

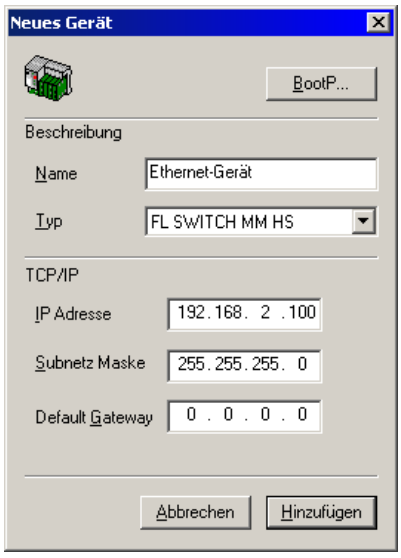


Bild 4-2 Eingabe-Maske der IP-Parameter

Achten Sie darauf, dass die Vergabe der IP-Parameter über BootP auch aktiviert ist.

Nachdem Sie auf „Hinzufügen“ geklickt haben, wird das Gerät in das Projekt eingefügt und ist als **nicht** erreichbar gekennzeichnet. Jetzt ist ein Neustart oder ein Reset des MMS erforderlich. Nach dem Neustart setzt der MMS wieder die BootP-Requests ab und erhält vom Factory Manager den entsprechenden BootP-Reply. Nach Abschluss des Boot-Vorgangs ist der MMS als erreichbar gekennzeichnet.

Falls der MMS jetzt immer noch als „nicht erreichbar“ gilt, sollten Sie die Einstellungen Ihrer Netzwerkkarte überprüfen. Beachten Sie, dass sich beide Teilnehmer im selben Netzwerk / Subnetz befinden müssen. Dass der Factory Manager die BootP-Requests empfängt, heißt nicht, dass die Geräte sich im selben Subnetz befinden, da die BootP-Requests als Broadcast über Subnetzgrenzen hinweg übertragen werden.

4.1.3 Konfiguration und Diagnose

Im Menü „Gerät“ finden Sie unter „Eigenschaften“ vielfältige Möglichkeiten zur Konfiguration und Diagnose des MMS.

Allgemeines

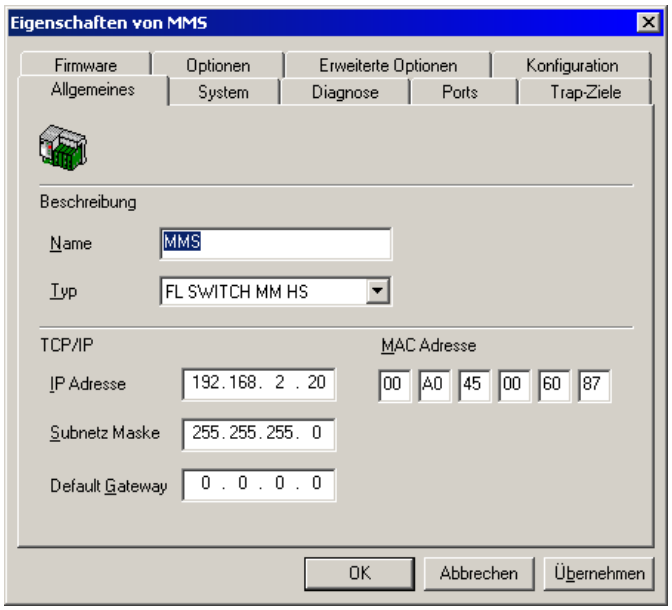


Bild 4-3 Menü „Allgemeines“

Hier können Gerätenamen und -typ sowie die IP-Parameter überprüft oder verändert werden.

Falls Sie die IP-Adresse und/oder die übrigen IP-Parameter über den Factory Manager verändern, haben Sie ab dem Moment, in dem Sie auf „OK“ klicken, keinen Zugriff mehr über den Factory Manager. Ein Neustart des MMS aktiviert die geänderten IP-Parameter, so dass der Zugriff wieder möglich ist.

Um die neuen Adressen nach einem Neustart zu aktivieren, muss BootP im MMS aktiviert sein (im WBM auf der Seite „IP Configuration“).

System

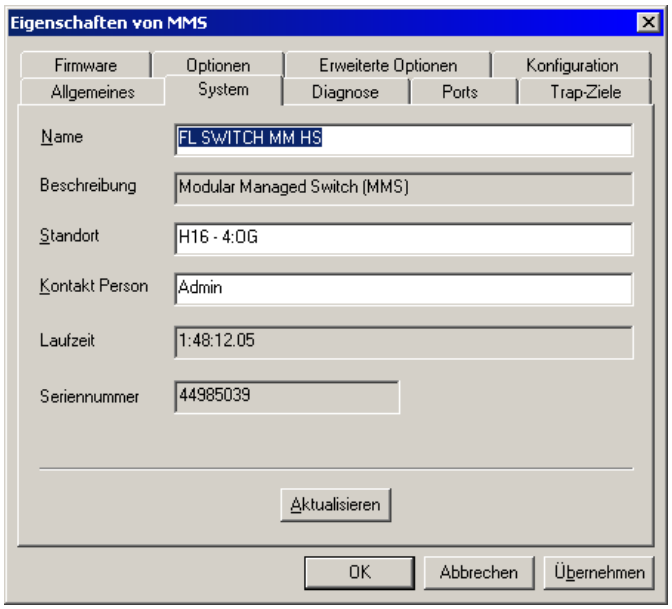


Bild 4-4 Menü „System“

In diesem Menü können Sie in den weiß hinterlegten Feldern weitere Informationen hinterlegen, die auf dem MMS abgespeichert werden. Diese Informationen stehen dann auch über SNMP und WBM zur Verfügung.

Diagnose

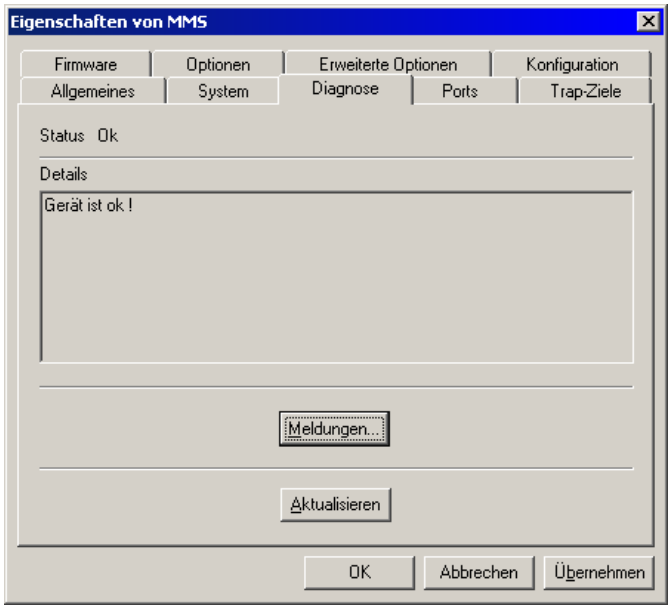


Bild 4-5 Menü „Diagnose“

Hier werden Details zum Gerätestatus und zur Redundanz angezeigt. Unter Meldungen werden alle Meldungen dieses Gerätes angezeigt.

Ports

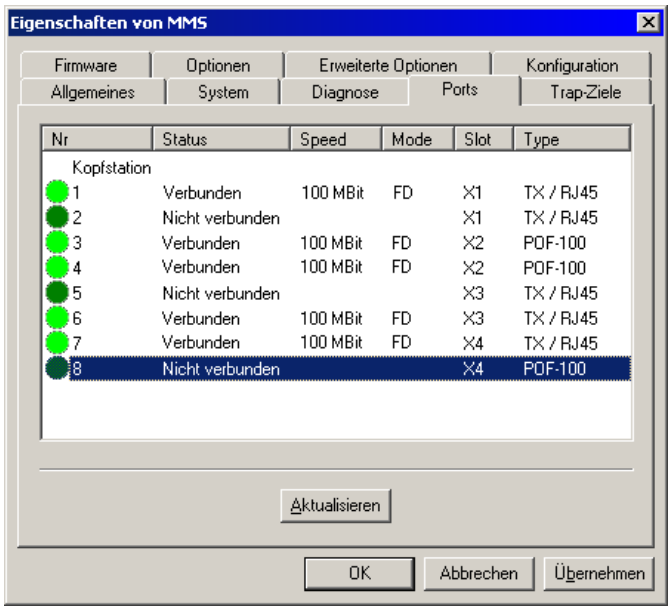


Bild 4-6 Menü „Ports“

Hier werden umfangreiche Informationen, wie z. B. über Interface-Typen, Stati und Übertragungsdaten, bis auf Port-Ebene dargestellt. Alle Informationen werden automatisch erstellt und aktualisiert.

Trap-Ziele

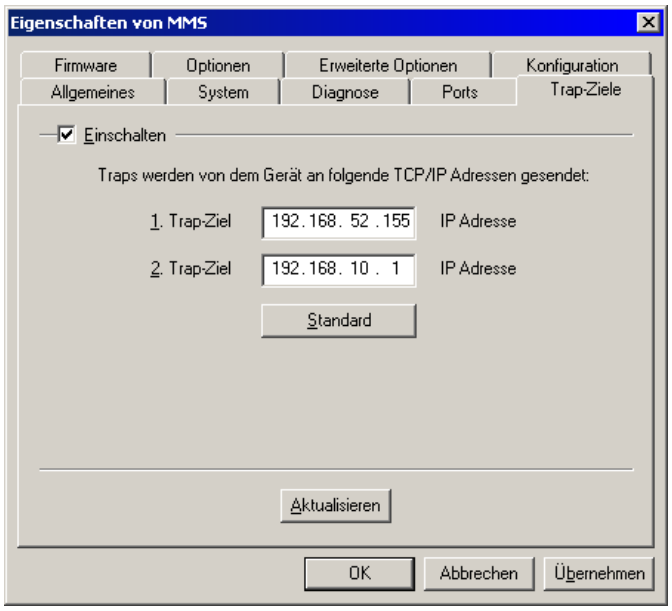


Bild 4-7 Menü „Trap-Ziele“

Hier werden die Trap-Ziele angezeigt oder eingestellt, sowie der Versand von Traps aktiviert/deaktiviert. Durch einen Klick auf „Standard“ wird die IP-Adresse des Rechners, auf dem der Factory Manager installiert ist, automatisch als Trap-Ziel aktiviert.

Firmware

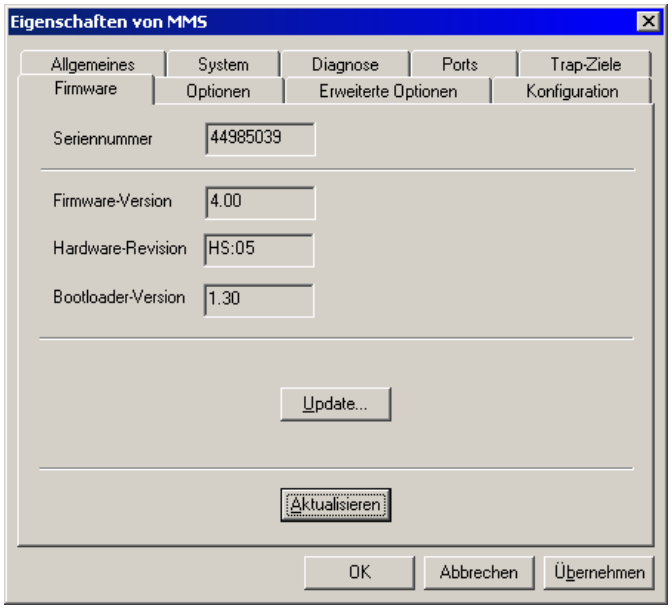


Bild 4-8 Menü „Firmware“

Hier erhalten Sie alle Informationen über die aktuelle Geräte-Software (Firmware). Außerdem besteht die Möglichkeit, ein Update der Software/Firmware mit Hilfe des Factory Managers vorzunehmen.

Firmware-Update

Wenn Sie auf Update klicken, erhalten Sie über nachfolgendes Fenster weitere Informationen zur verwendeten Firmware.

Bei einem Firmware-Update können Sie den Status auf dem Display des MMS verfolgen:

03 - Download der Firmware über das Netzwerk.

04 - Speichern der Firmware im Flash des MMS.

05 - Die neue Firmware wurde erfolgreich gespeichert.

Anzeige erlischt.

bo - Gerät bootet und lädt die neue Firmware ins RAM.

Nach einem Firmware-Update wird **automatisch** ein Reset durchgeführt, damit die neue Firmware aktiviert wird.

Vergewissern Sie sich, dass das Dienstprogramm „TFTP Server“ in der Toolbar aktiviert ist.

Sie können den Download im Meldungsfenster kontrollieren (25 %, 50 %, 75 %, 100 %). Warten Sie in jedem Fall, bis nach ungefähr zwei Minuten alle LEDs leuchten und das Gerät nach dem Booten wieder erreichbar ist.

Bei einem Firmware-Update ist nicht sichergestellt, dass alle vorhandenen Konfigurationsdaten nach dem Update / Downgrade erhalten bleiben. Überprüfen Sie daher die Konfigurationseinstellungen oder setzen Sie das Gerät in den Auslieferungszustand zurück.

Ein Spannungsausfall während eines Firmware-Updates führt dazu, dass die Firmware auf dem MMS zerstört wird. Ein Update über XMODEM ist erforderlich, siehe „Start mit defekter Software (Firmware)“ auf Seite 4-125.

Update

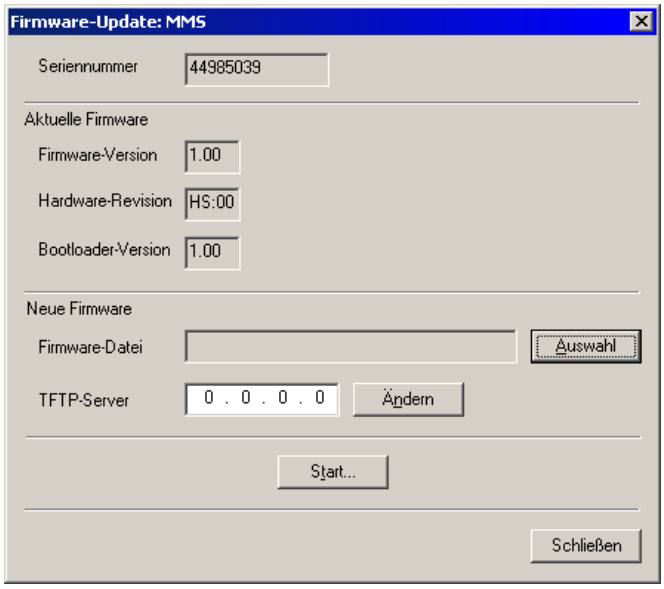


Bild 4-9 Menü „Update“

Damit ein Firmware-Update möglich ist, muss sich das Firmware-Image im Verzeichnis „Download“ des Factory Managers befinden.

Im Download-Center unter www.download.phoenixcontact.com finden Sie einen Anwenderhinweis zum Firmware-Update über TFTP (AH DE TFTP FIRMWARE UPDATE).

Optionen

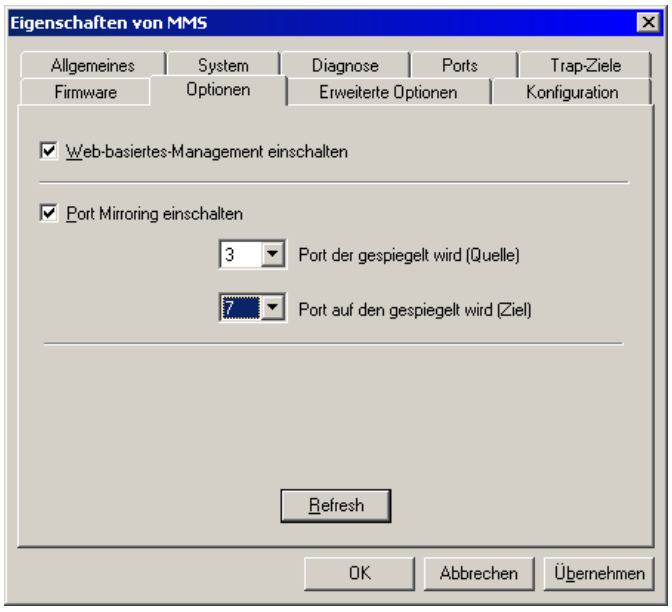


Bild 4-10 Menü „Optionen“

Zwei Funktionen stehen hier zur Auswahl:

– Aktivieren/Deaktivieren des Webservers.
– Konfigurieren der Port-Mirroring-Funktion.

Das Einstellen gleicher Ports für Quelle und Ziel hat zur Folge, dass das Port-Mirroring abgeschaltet wird. Der Source-Port wird auf „0“ gesetzt.

Um Multicast-Datenpakete auch am eingestellten Zielport empfangen zu können, muss der Zielport in die entsprechenden Multicast-Gruppen eingefügt werden.

Erweiterte Optionen

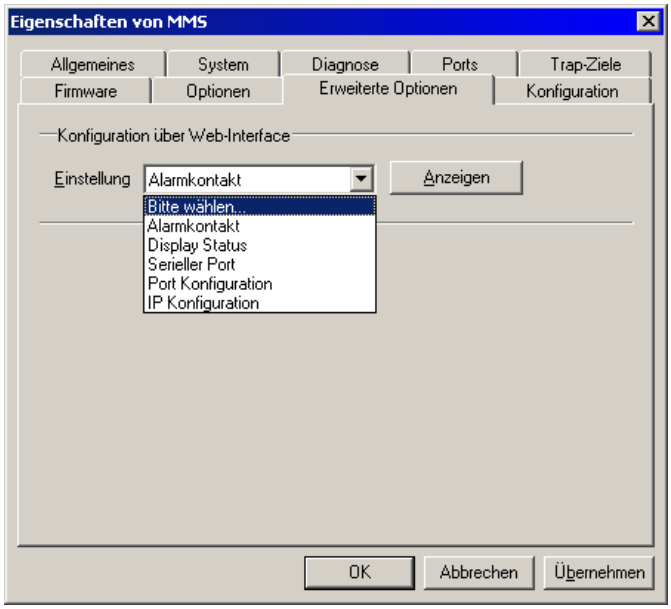


Bild 4-11 Menü „Erweiterte Optionen“

Von hier aus können Sie über ein Auswahl-Menü direkt ins Web-Interface springen. Die jeweilige Funktion ist in „Web Based Management - WBM“ auf Seite 4-11ff beschrieben.

Konfiguration

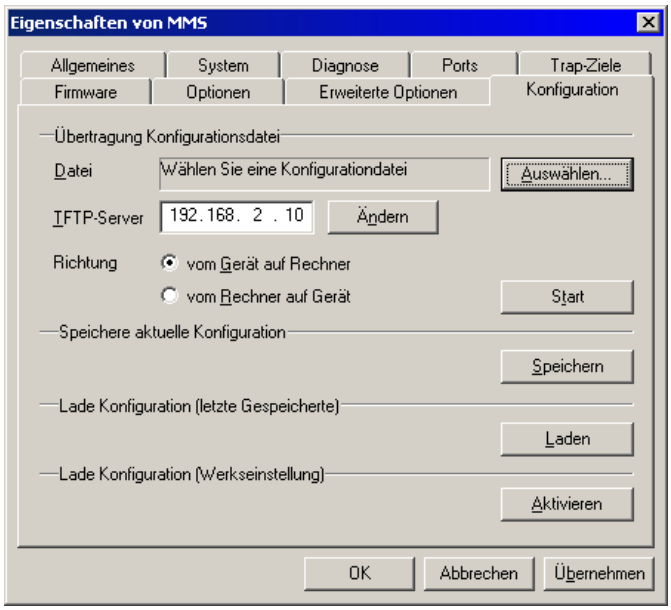


Bild 4-12 Menü „Konfiguration“

Die verschiedenen Varianten der Konfigurations-Speicherung oder des Konfigurations-Aufrufs stehen hier zur Auswahl.

4.2 Web Based Management - WBM

4.2.1 Allgemeine Funktion

Online-Diagnose

Über das komfortable Web-Based-Management-Interface haben Sie die Möglichkeit, den Switch von jedem Ort im Netz mit einem Standard-Browser zu managen. Umfangreiche Konfigurations- und Diagnose-Funktionen sind übersichtlich auf einer grafischen Bedienoberfläche dargestellt. Jeder Anwender kann - eine Netzwerkverbindung zum Gerät vorausgesetzt - über einen Browser lesend auf das Gerät zugreifen. Entsprechend dem physikalischen Aufbau des Switches sind so verschiedenste Informationen zum Gerät selber, zu den eingestellten Parametern und zum Betriebszustand einsehbar.

Veränderungen können nur in Verbindung mit dem gültigen Passwort vorgenommen werden. Im Auslieferungszustand lautet es „private“.

Aus Sicherheitsgründen wird die Änderung auf ein neues, nur Ihnen bekanntes Passwort empfohlen.

4.2.2 Voraussetzungen für die Verwendung des WBM

Da der Webserver über das Hyper Text Transfer Protocol arbeitet, ist die Verwendung eines Standard-Browsers ausreichend. Der Aufruf erfolgt über die URL „http://IP-Adresse des Gerätes“.
Beispiel: „http://172.16.29.112“.
Für die vollständige Bedienung der Webseiten ist die Unterstützung von Javascript 1.2 und von Cascading Style Sheets Level 1 erforderlich. Empfohlen wird die Verwendung des Microsoft Internet Explorers 6.0.

Der Aufruf des WBM kann nur über eine gültige IP-Adresse erfolgen. Im Auslieferungszustand verfügt der Switch über **keine** gültige IP-Adresse.

Vorgenommene Einstellungen werden nicht automatisch dauerhaft gespeichert. Falls die aktuelle Konfiguration nicht gespeichert wurde, erscheint im WBM rechts oben ein blinkendes Diskettensymbol. Das Symbol ist mit der Web-Seite „Configuration Management“ verlinkt. Über diese Web-Seite ist eine dauerhafte Speicherung der jetzigen Konfiguration mit „save current configuration“ möglich.

4.2.2.1 Aufbau der Webseiten

Die Webseiten sind in vier Bereiche geteilt:

– Gerätetyp und Gerätelogo.
– Gerätename (durch den Anwender vergeben) und Ladezeitpunkt, um Verwechselungen zu vermeiden.
– Navigationsbaum auf der linken Seite.
– Informationstabellen, die zur Laufzeit mit den aktuellen Geräteinformationen gefüllt werden.

4.2.2.2 Passwort-Konzept

Nach Eingabe des gültigen Passworts ist für die Zeitspanne von 300 s (Default) keine weitere Eingabe des Passworts erforderlich. Nach Ablauf dieser Zeit oder nach Betätigen des Buttons „Logout“ muss das Passwort erneut eingegeben werden.

Die Zeitspanne kann mit dem SNMP-Object „flWorkFWCtrlLoginExpire“ in dem Bereich von 30 s bis 3600 s eingestellt werden (Default 300 s).

Das Konzept greift für die ersten zehn gleichzeitig eingeloggten User. Alle weiteren User müssen jede Konfigurationsänderung solange jeweils mit dem Passwort bestätigen, bis weniger als zehn User angemeldet sind.

4.2.3 Funktionen / Informationen im WBM

Der Navigationsbaum bietet den direkten Zugriff auf folgende vier Bereiche:

– **General Instructions**
  Grundsätzliche Informationen zum WBM.
– **Device Information**
  Allgemeine Geräteinformationen.
– **General Configuration**
  Gerätekonfiguration / Gerät als Netzwerkteilnehmer.
– **Switch Station**
  Gerätespezifische Konfiguration und Diagnose.

4.2.3.1 General Instructions

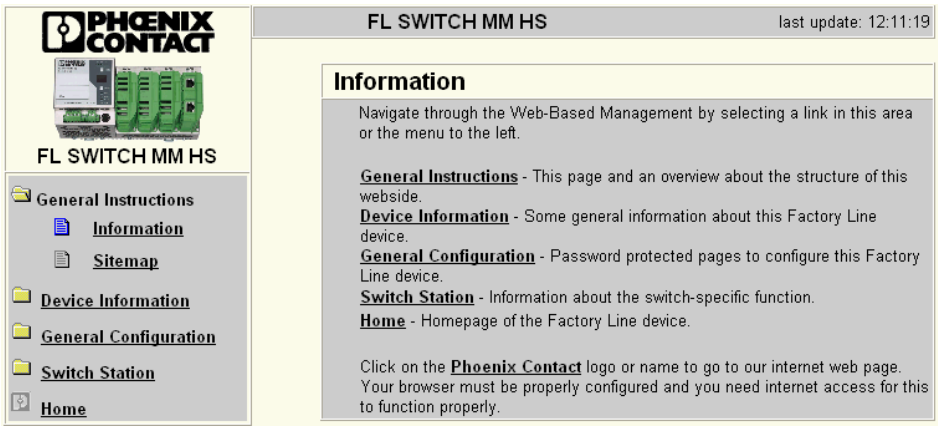

FL SWITCH MM HS
last update: 12:11:19
FL SWITCH MM HS
General Instructions
Information
Sitemap
Device Information
General Configuration
Switch Station
Home
Information
Navigate through the Web-Based Management by selecting a link in this area or the menu to the left.
General Instructions - This page and an overview about the structure of this webside.
Device Information - Some general information about this Factory Line device.
General Configuration - Password protected pages to configure this Factory Line device.
Switch Station - Information about the switch-specific function.
Home - Homepage of the Factory Line device.
Click on the Phoenix Contact logo or name to go to our internet web page. Your browser must be properly configured and you need internet access for this to function properly.

Bild 4-13 Webseite „Information“ beim MMS

General Instructions

Enthält eine kurze Beschreibung des WBMs, sowie einen Navigations-Baum (Sitemap), mit dem jede Seite des WBMs verlinkt ist.

4.2.3.2 Device Information

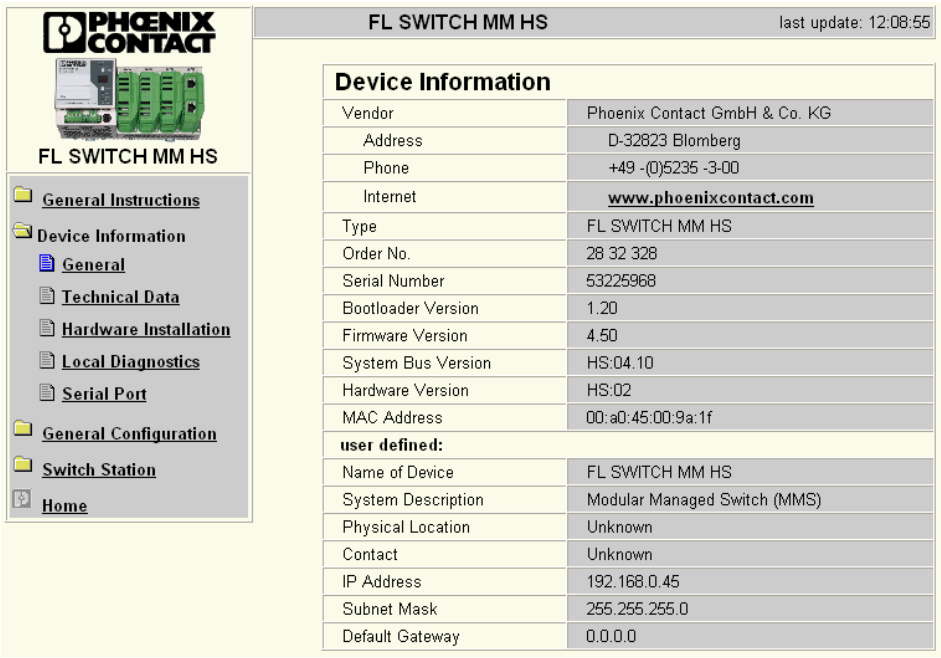


Bild 4-14 Webseite „Device Information“

Menü „General“
Hier finden Sie die verschiedensten statischen Informationen zum Gerät und zum Hersteller.

Menü „Technical Data“
Hier finden Sie eine Zusammenstellung der wichtigsten technischen Daten.

Menü „Hardware Installation“
Hier finden Sie eine Anschlussgrafik zum Anschluss der redundanten Spannungsversorgung und des Meldekontakts.

Menü „Local Diagnostics“
Hier finden Sie eine Beschreibung zur Bedeutung der umschaltbaren Diagnose- und Status-Anzeigen, außerdem werden die verschiedenen Anzeigemöglichkeiten der 7-Segment-Anzeige aufgeführt.

Menü „Serial Port“
Hier werden die Übertragungsparameter für die serielle Kommunikation genannt.

4.2.3.3 General Configuration

Menü „IP Configuration“
Hier sehen Sie, welche IP-Parameter, welche Management-VLAN-ID und welcher Adressierungsmechanismus eingestellt sind.

Die Management VLAN-ID gibt an, in welchem VLAN der Switch selbst zu erreichen ist, wenn er im VLAN-Modus „Tagging“ arbeitet.

Um die IP-Parameter über das WBM zu ändern, muss die Auswahl „Static“ aktiviert sein.

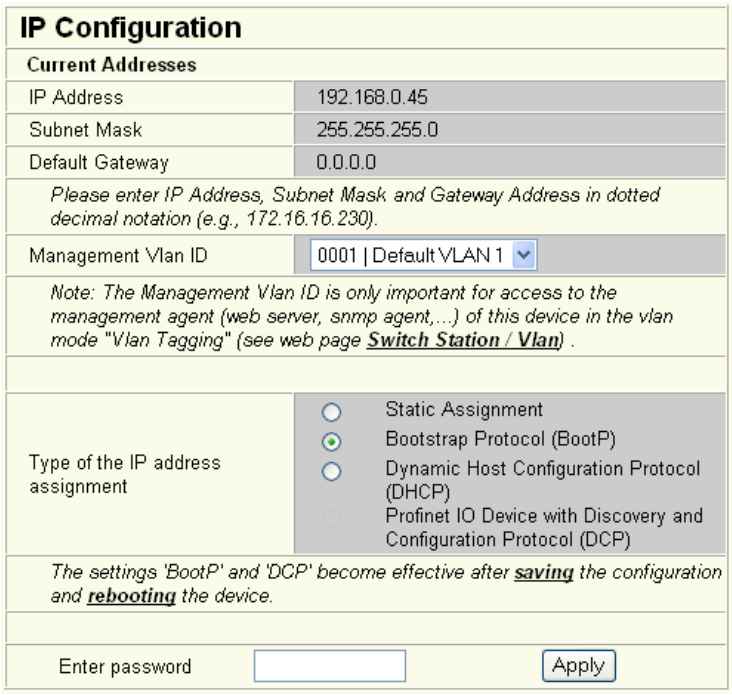

IP Configuration
Current Addresses
IP Address
192.168.0.45
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
Please enter IP Address, Subnet Mask and Gateway Address in dotted decimal notation (e.g., 172.16.16.230).
Management Vlan ID
0001 | Default VLAN 1
Note: The Management Vlan ID is only important for access to the management agent (web server, snmp agent,...) of this device in the vlan mode "Vlan Tagging" (see web page Switch Station / Vlan) .
Type of the IP address assignment
Static Assignment
Bootstrap Protocol (BootP)
Dynamic Host Configuration Protocol (DHCP)
Profinet IO Device with Discovery and Configuration Protocol (DCP)
The settings 'BootP' and 'DCP' become effective after saving the configuration and rebooting the device.
Enter password
Apply

Bild 4-15 Webseite „IP Configuration“

IP-Adressvergabe

Solange der Switch auf die Zuweisung einer IP-Adresse wartet - „01“ oder „dP“ im Display - blinkt zusätzlich die über den Mode-Taster ausgewählte Mode-LED.

– Static Assignment
  Der Switch ist unter der eingestellten IP-Adresse erreichbar und versendet keinerlei Requests zum Erhalt von IP-Parametern.

Falls Sie die IP-Adresse und/oder die übrigen IP-Parameter über WBM verändern, haben Sie ab dem Moment, in dem Sie auf „Apply“ klicken, keinen Zugriff mehr über die im Browser eingestellte IP-Adresse.

– Bootstrap Protocol - BootP
  Der Switch versendet einen BootP-Request nach jedem Neustart und erhält einen BootP-Reply mit IP-Parametern. Bleibt der BootP-Reply aus, startet der Switch nach dem dritten Request mit den letzten gespeicherten IP-Parametern. Verfügt der Switch nicht über gespeicherte IP-Parameter, versendet der Switch solange BootP-Request bis diese mit einem BootP-Reply beantwortet werden.

– Dynamic Host Configuration Protocol - DHCP
  Nach dem Einschalten von DHCP versucht der Switch, Netzwerkparameter von einem DHCP Server zu beziehen. Die Einstellung, ob DHCP ein- oder ausgeschaltet ist, wird permanent gespeichert.

Nach dem Einschalten von DHCP zeigt das Display „01“ und wartet auf IP-Parameter von einem DHCP-Server. Solange keine IP-Parameter von einem DHCP-Server vergeben wurden, ist der Switch **weiterhin** über die zuvor eingestellten IP-Parameter erreichbar.

– Discovery and Configuration Protocol - DCP
  Modus zur Vergabe der IP-Adressen unter PROFINET. Der Switch wartet nach dem Starten auf die Inbetriebnahme durch einen IO-Controller oder ein Engineering-Werkzeug. Dieser Zustand wird durch die Display-Ausgabe „dP“ signalisiert. Der Switch ist nach der Konfiguration nur unter der zugewiesenen IP-Adresse erreichbar. Die zugewiesene IP-Adresse wird nicht permanent gespeichert, so dass der Switch bei jedem Gerätestart auf die Zuweisung einer Adresse wartet. DCP wird automatisch aktiviert, wenn die Betriebsart „Profinet“ gewählt wird.

Wenn der MMS eine PROFINET-Verbindung aufgebaut hat, zeigt das Display unten rechts einen Punkt.

Menü „System Identification“
In diesem Menü können Anwender-spezifische Gerätedaten, z. B. Standort, Gerätenamen oder Funktion, angezeigt oder verändert werden. Diese Gerätedaten stehen dann auch im SNMP zur Verfügung.

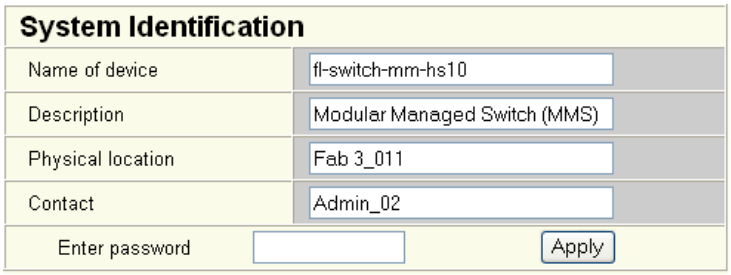
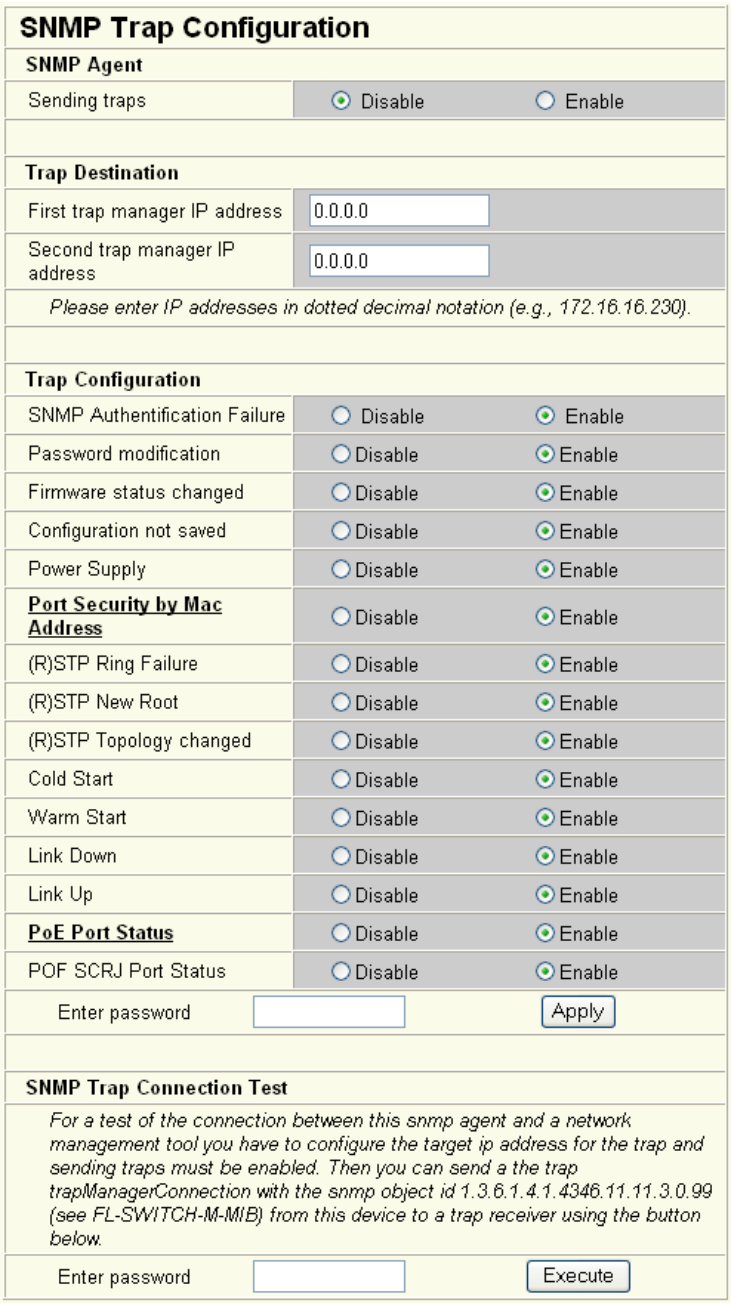


Bild 4-16 Menü „System Identification“

Menü „SNMP Trap Configuration“

SNMP Agent Hier kann der Versand von Traps global ein-/ausgeschaltet werden.



SNMP Trap Configuration

SNMP Agent		
Sending traps	(•) Disable	( ) Enable
Trap Destination		
First trap manager IP address	0.0.0.0	
Second trap manager IP address	0.0.0.0	
Please enter IP addresses in dotted decimal notation (e.g., 172.16.16.230).		
Trap Configuration		
SNMP Authentification Failure	( ) Disable	(•) Enable
Password modification	( ) Disable	(•) Enable
Firmware status changed	( ) Disable	(•) Enable
Configuration not saved	( ) Disable	(•) Enable
Power Supply	( ) Disable	(•) Enable
Port Security by Mac Address	( ) Disable	(•) Enable
(R)STP Ring Failure	( ) Disable	(•) Enable
(R)STP New Root	( ) Disable	(•) Enable
(R)STP Topology changed	( ) Disable	(•) Enable
Cold Start	( ) Disable	(•) Enable
Warm Start	( ) Disable	(•) Enable
Link Down	( ) Disable	(•) Enable
Link Up	( ) Disable	(•) Enable
PoE Port Status	( ) Disable	(•) Enable
POF SCRJ Port Status	( ) Disable	(•) Enable
Enter password		Apply
SNMP Trap Connection Test		
For a test of the connection between this snmp agent and a network management tool you have to configure the target ip address for the trap and sending traps must be enabled. Then you can send a the trap trapManagerConnection with the snmp object id 1.3.6.1.4.1.4346.11.11.3.0.99 (see FL-SWITCH-M-MIB) from this device to a trap receiver using the button below.		
Enter password		Execute

Bild 4-17 Webseite „SNMP Configuration“

Trap Destination In diesem Bereich der Tabelle können Sie die IP-Adressen der zwei Trap-Receiver lesen oder verändern.

Trap Configuration Hier können Sie den Versand der Traps einzeln abschalten.

SNMP Trap Connection Test

Nachdem Sie den Versand von Traps aktiviert haben und mit Hilfe der IP-Adressen die Trap-Manager definiert haben, können Sie jetzt mit dem „Execute“-Button Test-Traps versenden, um den Kommuniaktionsweg vom Switch zum Trap-Receiver zu testen.

Menü „Software Update“

Hier können Sie die Parameter für ein Software-Update lesen oder verändern und das Update auslösen.

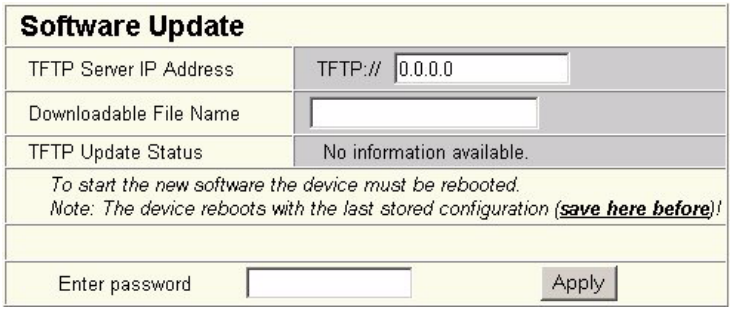

Software Update
TFTP Server IP Address
TFTP:// 0.0.0.0
Downloadable File Name
TFTP Update Status
No information available.
To start the new software the device must be rebooted.
Note: The device reboots with the last stored configuration (save here before)!
Enter password
Apply

Bild 4-18 Webseite „Software Update“

Bei einem Firmware-Update können Sie den Status auf dem Display des MMS verfolgen:

03 - Download der Firmware über das Netzwerk.

04 - Speichern der Firmware im Flash des MMS.

05 - Die neue Firmware wurde erfolgreich gespeichert.

Anzeige erlischt.

bo - Gerät bootet und lädt die neue Firmware ins RAM.

Nach einem Firmware-Update wird wahlweise **automatisch** ein Reset durchgeführt, damit die neue Firmware aktiviert wird.

Vergewissern Sie sich, dass das Dienstprogramm „TFTP Server“ in der Toolbar des Factory Managers aktiviert ist.

Sie können den Download im Meldungsfenster des Factory Managers kontrollieren (25 %, 50 %, 75 %, 100 %). Warten Sie in jedem Fall, bis nach ungefähr zwei Minuten alle LEDs leuchten und das Gerät nach dem Booten wieder erreichbar ist.

Beim einen Firmware-Update ist nicht sichergestellt, dass alle vorhandenen Konfigurationsdaten nach dem Update / Downgrade erhalten bleiben. Überprüfen Sie daher die Konfigurationseinstellungen oder setzen Sie das Gerät in den Auslieferungszustand zurück.

Ein Spannungsausfall während eines Firmware-Updates führt dazu, dass die Firmware auf dem MMS zerstört wird. Ein Update über XMODEM ist erforderlich, siehe „Start mit defekter Software (Firmware)“ auf Seite 4-125.

Menü „Change Password“

Hier können Sie unter Angabe des aktuellen Passworts ein neues, nur Ihnen bekanntes Passwort vergeben. Im Auslieferungszustand lautet das Passwort „private“ (Groß-/Kleinschreibung beachten). Aus Sicherheitsgründen wird in den Eingabefeldern nicht Ihr Passwort, sondern „*******“ angezeigt.

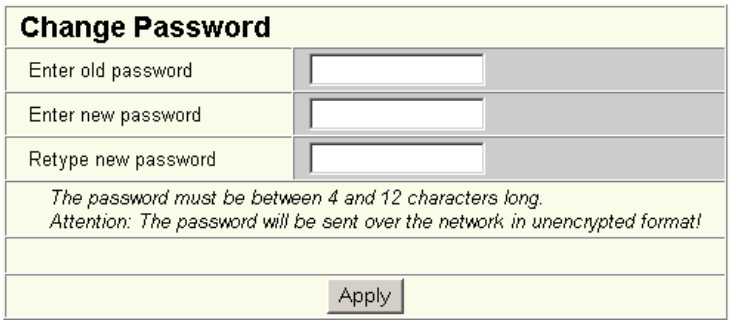

Change Password
Enter old password
Enter new password
Retype new password
The password must be between 4 and 12 characters long.
Attention: The password will be sent over the network in unencrypted format!
Apply

Bild 4-19 Webseite „Change Passwort“

Das Passwort muss zwischen vier und zwölf Zeichen lang sein. Beachten Sie, dass das Passwort stets unverschlüsselt über das Netzwerk übertragen wird.

Passwort vergessen?!
Halten Sie die Seriennummer und die MAC-Adresse des Gerätes bereit, bevor Sie die im Anhang genannte Telefonnummer von Phoenix Contact wählen.

Menü „User Interfaces“

Hier können Sie folgende Aktionen durchführen:

– Aktivieren/Deaktivieren des Telnet-Servers.
– Aktivieren/Deaktivieren des Web-Servers.
– Aktivieren/Deaktivieren des SNMP-Agenten.
– Aktivieren/Deaktivieren der Konfigurationsseiten für die Redundanzmechanismen.
– Aktivieren/Deaktivieren der Konfigurationsseiten für Multicast Filtering.
– Aktivieren/Deaktivieren der Konfigurationsseiten für VLAN.
– Aktivieren/Deaktivieren der Konfigurationsseiten für den DHCP Relay Agent.

Mit der Aktivierung/Deaktivierung der Konfigurationsseiten unter „User Interfaces“ werden nur im WBM-Menü die Webseiten zur Konfiguration der gewählten Funktionen frei- oder abgeschaltet.

– Einstellung des Refresh-Intervalls für die automatische Aktualisierung der Web-Seiten. Sie können hier das Refresh-Intervall für die automatische Aktualisierung verschiedener Webseiten einstellen. Falls Sie das Intervall auf „0“ setzen, werden die Seiten nicht mehr aktualisiert.

Die automatische Aktualisierung der Webseiten funktioniert nur mit dem Internet Explorer ab der Version 5.5.

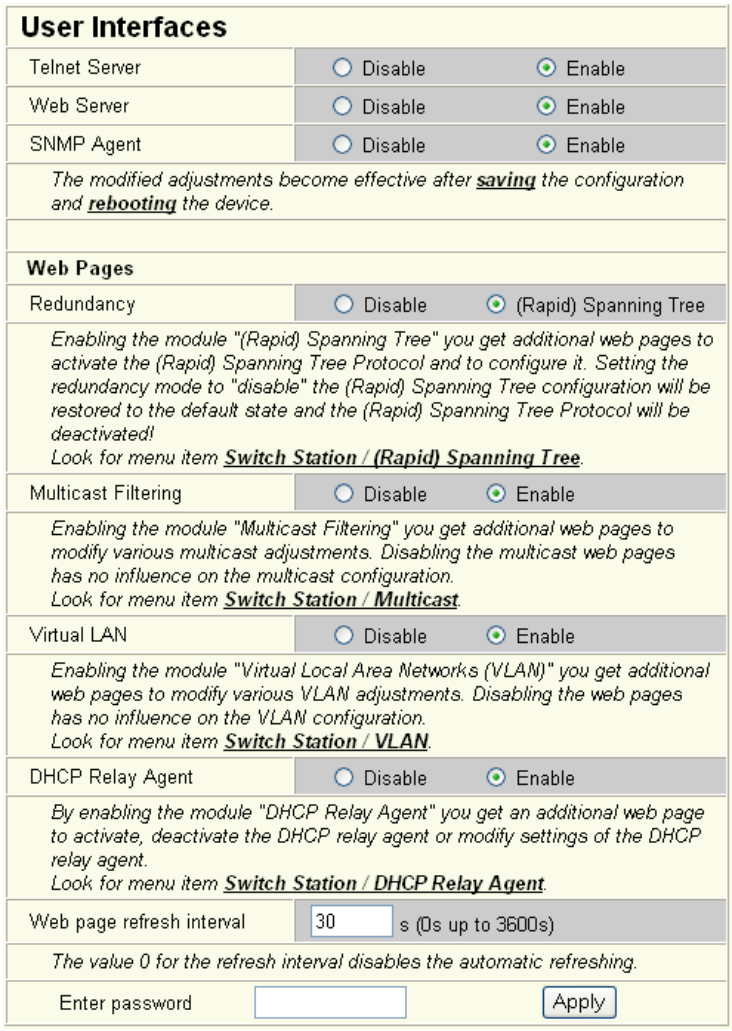

User Interfaces
Telnet Server
Disable
Enable
Web Server
Disable
Enable
SNMP Agent
Disable
Enable
The modified adjustments become effective after saving the configuration and rebooting the device.
Web Pages
Redundancy
Disable
(Rapid) Spanning Tree
Enabling the module "(Rapid) Spanning Tree" you get additional web pages to activate the (Rapid) Spanning Tree Protocol and to configure it. Setting the redundancy mode to "disable" the (Rapid) Spanning Tree configuration will be restored to the default state and the (Rapid) Spanning Tree Protocol will be deactivated!
Look for menu item Switch Station / (Rapid) Spanning Tree.
Multicast Filtering
Disable
Enable
Enabling the module "Multicast Filtering" you get additional web pages to modify various multicast adjustments. Disabling the multicast web pages has no influence on the multicast configuration.
Look for menu item Switch Station / Multicast.
Virtual LAN
Disable
Enable
Enabling the module "Virtual Local Area Networks (VLAN)" you get additional web pages to modify various VLAN adjustments. Disabling the web pages has no influence on the VLAN configuration.
Look for menu item Switch Station / VLAN.
DHCP Relay Agent
Disable
Enable
By enabling the module "DHCP Relay Agent" you get an additional web page to activate, deactivate the DHCP relay agent or modify settings of the DHCP relay agent.
Look for menu item Switch Station / DHCP Relay Agent.
Web page refresh interval
30
s (0s up to 3600s)
The value 0 for the refresh interval disables the automatic refreshing.
Enter password
Apply

Bild 4-20 Webseite „User Interfaces“

Menü „Access Control“

Hier können Sie vorgeben, von welchen IP-Adressen aus der Zugriff auf das Web-Interface gestattet ist. Geben Sie dazu die IP-Adresse als Dotted-Notation an und wählen Sie aus, ob Nur-Lese-Rechte oder Lese-Schreib-Rechte vergeben werden. Optional können Sie unter „Description“ noch einen Namen vergeben. Für maximal zehn IP-Adressen kann der Zugriff auf das WBM konfiguriert werden.

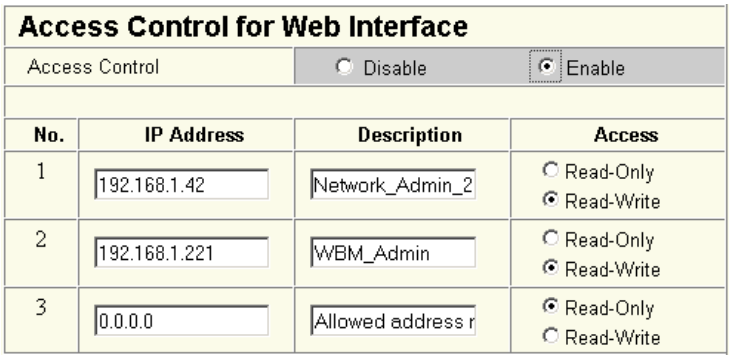


Bild 4-21 Webseite „Access Control for Web Interface“

Durch fehlerhafte Konfiguration ist es möglich, dass Sie sich selbst „aussperren“. In dem Falle kann über das **serielle** Interface mit Hilfe des Schalters „Access Control for Web“ der Zugriffsschutz wieder aufgehoben werden.

Menü „Operating Mode“

Betrieb als PROFINET-Device

In diesem Menü wählen Sie aus, ob der Switch als PROFINET-Device betrieben werden soll. Weitere Informationen zum Betrieb als PROFINET-Device finden Sie in Kapitel 9 „Betrieb als PROFINET-Device“.

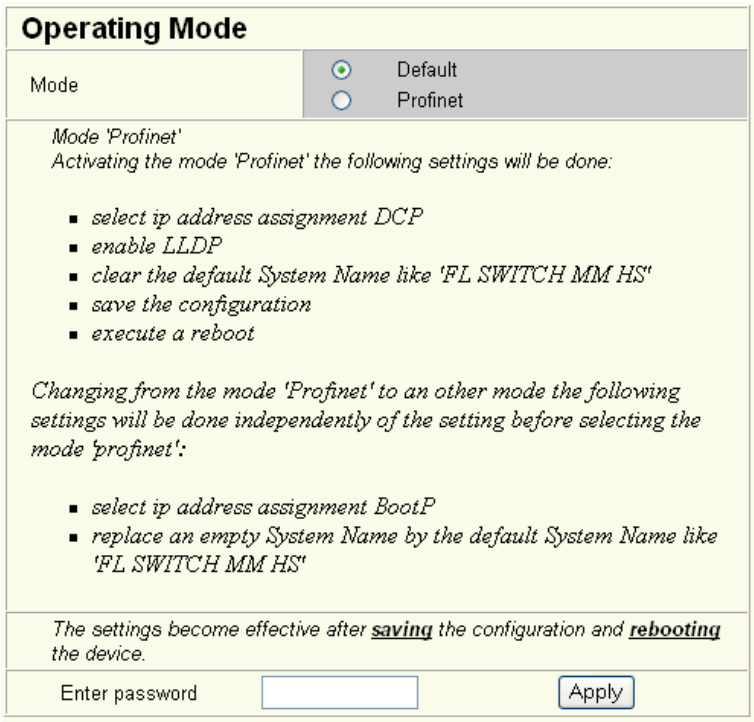

Operating Mode
Mode
Default
Profinet
Mode 'Profinet'
Activating the mode 'Profinet' the following settings will be done:
select ip address assignment DCP
enable LLDP
clear the default System Name like 'FL SWITCH MM HS'
save the configuration
execute a reboot
Changing from the mode 'Profinet' to an other mode the following settings will be done independently of the setting before selecting the mode 'profinet':
select ip address assignment BootP
replace an empty System Name by the default System Name like 'FL SWITCH MM HS'
The settings become effective after saving the configuration and rebooting the device.
Enter password
Apply

Bild 4-22 Webseite „Operating Mode“

Menü „Config. Management\General“
In dieser Tabelle können Sie alle Parameter, die zur Abspeicherung der aktuellen oder zum Laden einer neuen Konfiguration erforderlich sind, einsehen und unter Angabe des gültigen Passwortes verändern. Außerdem können Sie den Neustart mit der entsprechenden Konfiguration veranlassen.

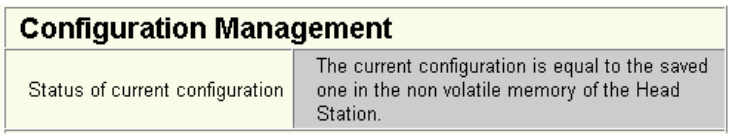

Configuration Management
Status of current configuration
The current configuration is equal to the saved one in the non volatile memory of the Head Station.

Bild 4-23 Webseite „Configuration Management“

Mögliche Stati von „Status of current configuration“:

– The configuration has been modified but not saved (zusätzliche Kennzeichnung durch blinkendes Diskettensysmbol).
– Saving the current configuration.
– The current configuration is equal to the saved one in the non volatile memory of the switch.
– The current configuration was saved.

Save current configuration

Hier können Sie die aktuelle Konfiguration mit dem zugehörigen Konfigurationsnamen unter Angabe des gültigen Passworts speichern.

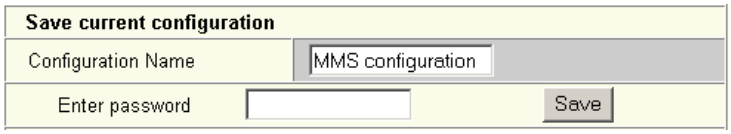


Bild 4-24 Webseite „Save current configuration“

Falls nach einem Konfigurations-Download die neue Konfiguration nicht durch einen Reset aktiviert wurde, überschreibt der Befehl „Save current configuration“ die zuvor geladene Konfiguration und speichert stattdessen die zurzeit aktive Konfiguration des MMS.

Set default upon delivery

Hier können Sie unter Angabe des gültigen Passwortes den Switch auf die Werkseinstellungen (Auslieferungszustand) zurücksetzen.

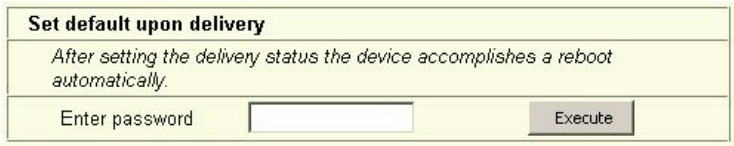

Set default upon delivery
After setting the delivery status the device accomplishes a reboot automatically.
Enter password
Execute

Bild 4-25 Webseite „Set default upon delivery“

Der Aufruf des WBM kann nur über eine gültige IP-Adresse erfolgen. Nach dem Rücksetzen auf die Werkseinstellungen, also in den Auslieferungszustand zurück, verfügt der Switch über **keine** IP-Adresse und der Adressierungsmechanismus ist auf BootP eingestellt.

Load the last stored configuration

Hiermit können Sie die letzte im Memory-Modul hinterlegte oder die auf dem Gerät gespeicherte Konfiguration erneut aktivieren. Damit gehen alle Konfigurationsänderungen seit dem letzten Speichern verloren.

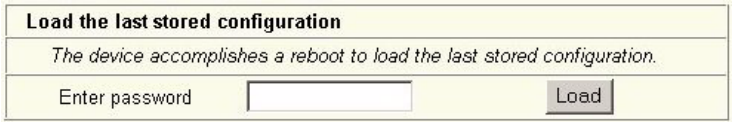

Load the last stored configuration
The device accomplishes a reboot to load the last stored configuration.
Enter password
Load

Bild 4-26 Webseite „Load the last stored configuration“

Menü „Config. Management/File Transfer“

Configuration file transfer

Hier können Sie Ihre Gerätekonfiguration auf einem PC sichern oder den Switch mit einer hinterlegten Konfiguration betreiben.

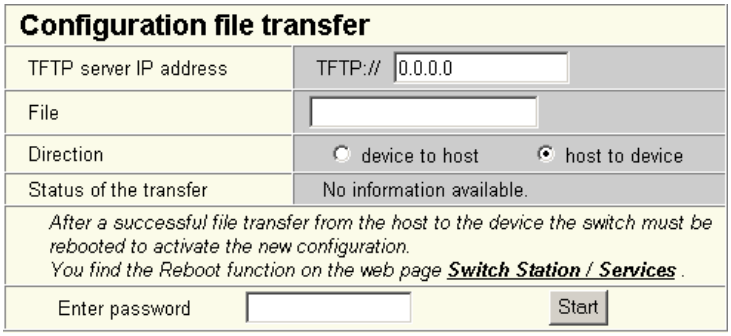

Configuration file transfer
TFTP server IP address
TFTP:// 0.0.0.0
File
Direction
device to host
host to device
Status of the transfer
No information available.
After a successful file transfer from the host to the device the switch must be rebooted to activate the new configuration.
You find the Reboot function on the web page Switch Station / Services .
Enter password
Start

Bild 4-27 Webseite „Configuration file transfer“

Bei einem Upload einer Konfiguration vom MMS auf einen PC wird die letzte gespeicherte Version übertragen. Um die aktuelle Konfiguration zu übertragen, ist es empfehlenswert, sie zuvor noch einmal zu speichern (Save current configuration).

Bei einem Download einer Konfiguration vom PC auf einen MMS wird die neue Konfiguration erst nach einem Reset des Switches aktiviert.

Die Verwendung einer Konfigurationsdatei hat keinen Einfluss auf ein bestehendes („altes“) Passwort.

Gerätetausch

Die Konfiguration über eine Konfigurationsdatei dient dem Gerätetausch. Sollen Geräte per Konfigurationsdatei dupliziert werden, müssen folgende Details beachtet werden:

– Aufbau einer Punkt-zu-Punkt-Verbindung zwischen einem MMS und der Management-Station.
– Konfigurationsdatei auf den MMS laden.
– Reset des MMS durchführen.
– IP-Parameter anpassen.
– Konfiguration speichern (Save current configuration).

Der duplizierte Switch kann nun mit den angepassten IP-Parametern im Netz betrieben werden.

Menü „Config. Management/Memory Module“

Auf dieser Webseite erhalten Sie einen Überblick über die Konfiguration im Memory-Modul und welche Konfiguration beim Booten verwendet wurde.

Memory Module

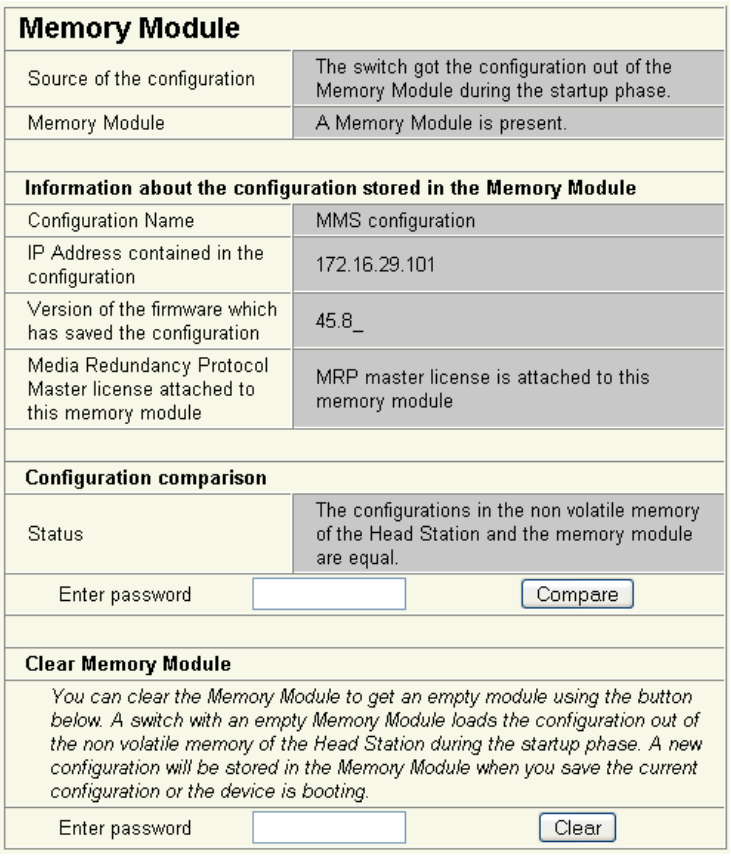

Memory Module
Source of the configuration
The switch got the configuration out of the Memory Module during the startup phase.
Memory Module
A Memory Module is present.
Information about the configuration stored in the Memory Module
Configuration Name
MMS configuration
IP Address contained in the configuration
172.16.29.101
Version of the firmware which has saved the configuration
45.8_
Media Redundancy Protocol Master license attached to this memory module
MRP master license is attached to this memory module
Configuration comparison
Status
The configurations in the non volatile memory of the Head Station and the memory module are equal.
Enter password
Compare
Clear Memory Module
You can clear the Memory Module to get an empty module using the button below. A switch with an empty Memory Module loads the configuration out of the non volatile memory of the Head Station during the startup phase. A new configuration will be stored in the Memory Module when you save the current configuration or the device is booting.
Enter password
Clear

Bild 4-28 Webseite „Memory Module“

Configuration comparison

Hier können Sie einen Vergleich zwischen der Konfiguration auf dem Memory-Modul und der Konfiguration im Speicher der Kopfstation durchführen lassen. Das Ergebnis wird als Text angezeigt. Außerdem zeigt das Display das Ergebnis codiert an (siehe auch Kapitel „Bedeutung der 7-Segment-Anzeige“ auf Seite 1-14).

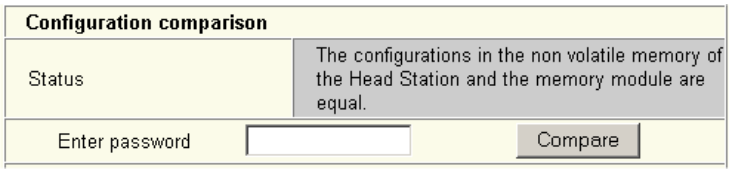

Configuration comparison
Status
The configurations in the non volatile memory of the Head Station and the memory module are equal.
Enter password
Compare

Bild 4-29 Webseite „Configuration comparison“

Falls Sie innerhalb weniger Sekunden ein Memory-Modul gegen ein anderes tauschen, muss der Konfigurations-Vergleich manuell aktualisiert werden.

Clear Memory Module

Hier können Sie das Memory-Modul unter Angabe des gültigen Passwortes löschen.

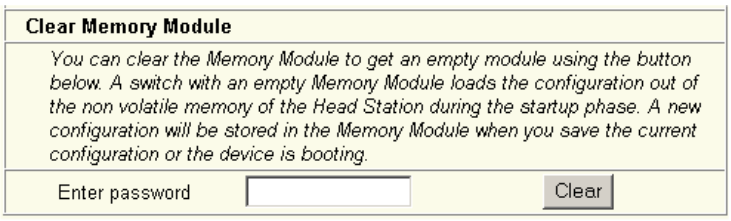

Clear Memory Module
You can clear the Memory Module to get an empty module using the button below. A switch with an empty Memory Module loads the configuration out of the non volatile memory of the Head Station during the startup phase. A new configuration will be stored in the Memory Module when you save the current configuration or the device is booting.
Enter password
Clear

Bild 4-30 Webseite „Clear Memory Module“

4.2.3.4 Switch Station

Menü „Services“

Reboot

Um einen Reboot über das Web-Interface auszulösen, ist die Eingabe des gültigen Passwortes erforderlich. Damit Konfigurationsänderungen erhalten bleiben oder durch einen Neustart aktiviert werden, speichern Sie voher die Konfiguration.

Port Security Status

Hier können Sie global die Port-Security-Funktion aktivieren bzw. deaktivieren. Die Einstellungen für einzelne Ports können Sie auf der Web-Seite „Port/Ports-Security“ vornehmen.

Illegal Address Counter

Hier können Sie den Zähler, der die unberechtigten Zugriffe auf das Gerät erfasst, zurücksetzen.

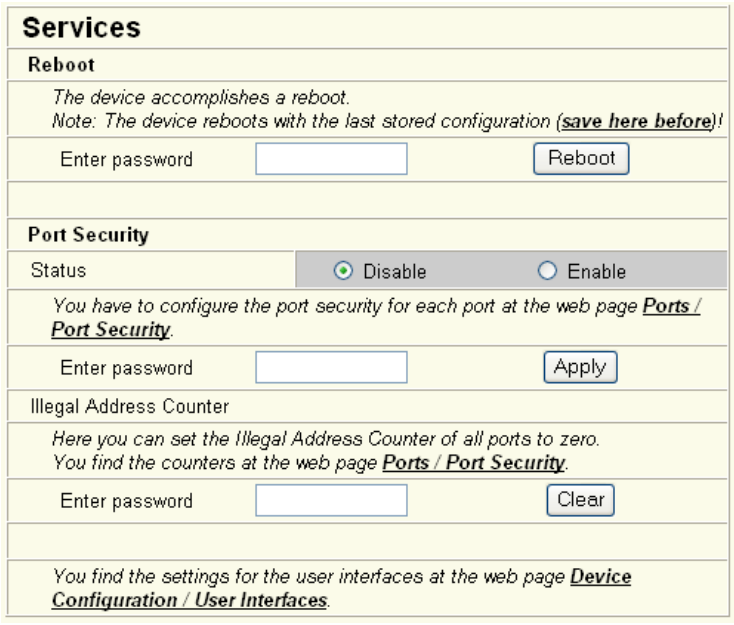

Services
Reboot
The device accomplishes a reboot.
Note: The device reboots with the last stored configuration (save here before)!
Enter password
Reboot
Port Security
Status
Disable
Enable
You have to configure the port security for each port at the web page Ports / Port Security.
Enter password
Apply
Illegal Address Counter
Here you can set the Illegal Address Counter of all ports to zero.
You find the counters at the web page Ports / Port Security.
Enter password
Clear
You find the settings for the user interfaces at the web page Device Configuration / User Interfaces.

Bild 4-31 Webseite „Services“

Menü „DHCP Relay Agent“

In diesem Menü kann der DHCP Relay Agent portbezogen aktiviert/deaktiviert , die zugehörige Adresse des DHCP-Servers eingetragen und der Typ der Remote-ID konfiguriert werden.

Weitere Informationen zur Funktion des DHCP Relay Agenten finden Sie im Kapitel „DHCP Relay Agent“ auf Seite 11-1.

Menü „Ports\Port Table“

Übersicht über alle verfügbaren Ports. Durch Klicken auf die entsprechende Portnummer wird eine Port-spezifische Seite (Port Configuration) geöffnet.

Port Table

Module	Interface	Port	Type	Port Status	Link State
HS	X1	1	TX 10/100	enable	100 MBit FD
		2	TX 10/100	enable	100 MBit FD
	X2	3	TX 10/100 MEM	enable	not connected
		4	TX 10/100 MEM	enable	not connected
	X3	5	empty	enable	not connected
		6	empty	enable	not connected
	X4	7	empty	enable	not connected
		8	empty	enable	not connected

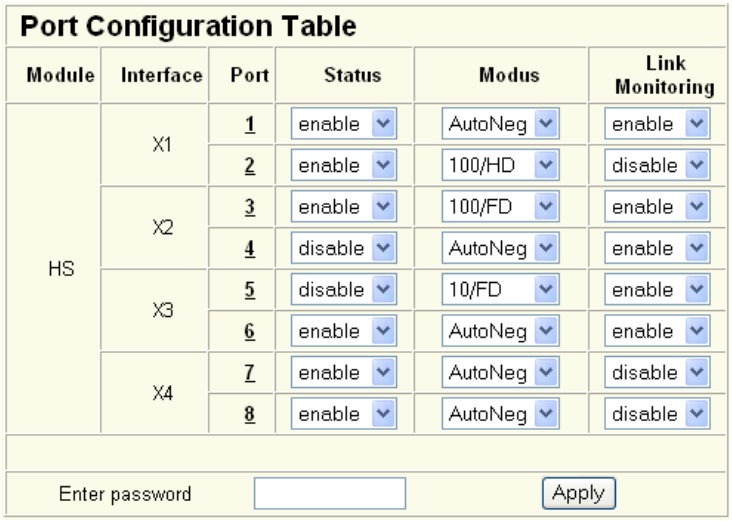
Note: This web page will be refreshed in 20 sec automatically (change the interval at the web page 'Services')!

Bild 4-32 Webseite „Port Table“

Achten Sie bei der Einstellung des Übertragungsmodus darauf, dass an beiden Seiten der Verbindung die gleichen Einstellungen vorgenommen werden. Eine ungleiche Einstellung kann zu vermehrten Kollisionen oder CRC-Fehlern führen und die Performance des Netzwerkes beeinträchtigen.

Menü „Ports\Port Cfg. Table“

Dieses Menü bietet eine übersichtliche Darstellung wichtiger Konfigurationseinstellungen aller Ports und bietet zusätzlich die Möglichkeit, den Status, den Übertragungsmodus und die Link-Überwachung für alle vorhandenen Ports einzustellen.



Port Configuration Table

Module	Interface	Port	Status	Modus	Link Monitoring
HS	X1	1	enable	AutoNeg	enable
		2	enable	100/HD	disable
	X2	3	enable	100/FD	enable
		4	disable	AutoNeg	enable
	X3	5	disable	10/FD	enable
		6	enable	AutoNeg	enable
	X4	7	enable	AutoNeg	disable
		8	enable	AutoNeg	disable

Enter password Apply

Bild 4-33 Webseite „Port Configuration Table“

Menü „Ports\Port Configuration“

Bietet individuelle Konfigurations-Möglichkeiten jedes einzelnen Ports.

Auch bei abgeschaltetem Port bleibt die Link-LED des Ports aktiv.

.

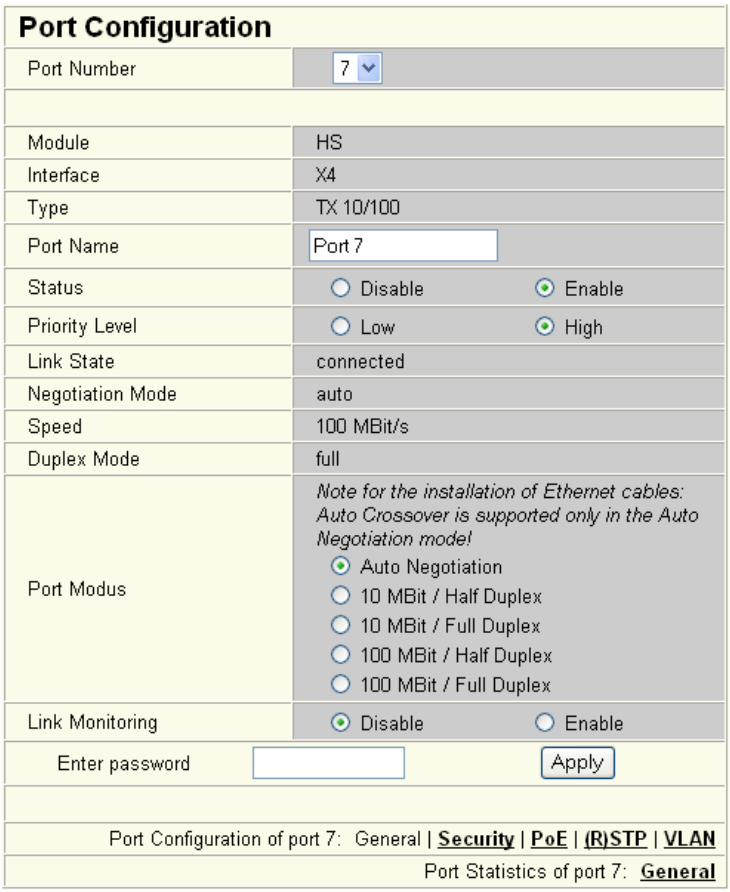


Bild 4-34 Webseite „Port Configuration“

Menü „Ports\Port Statistics“

Dieses Menü bietet detaillierte Statistikinformationen über das Datenaufkommen jedes einzelnen Ports. Auf dieser Seite können zusätzliche Zählerstände von allen Ports auf Null gesetzt werden.

.

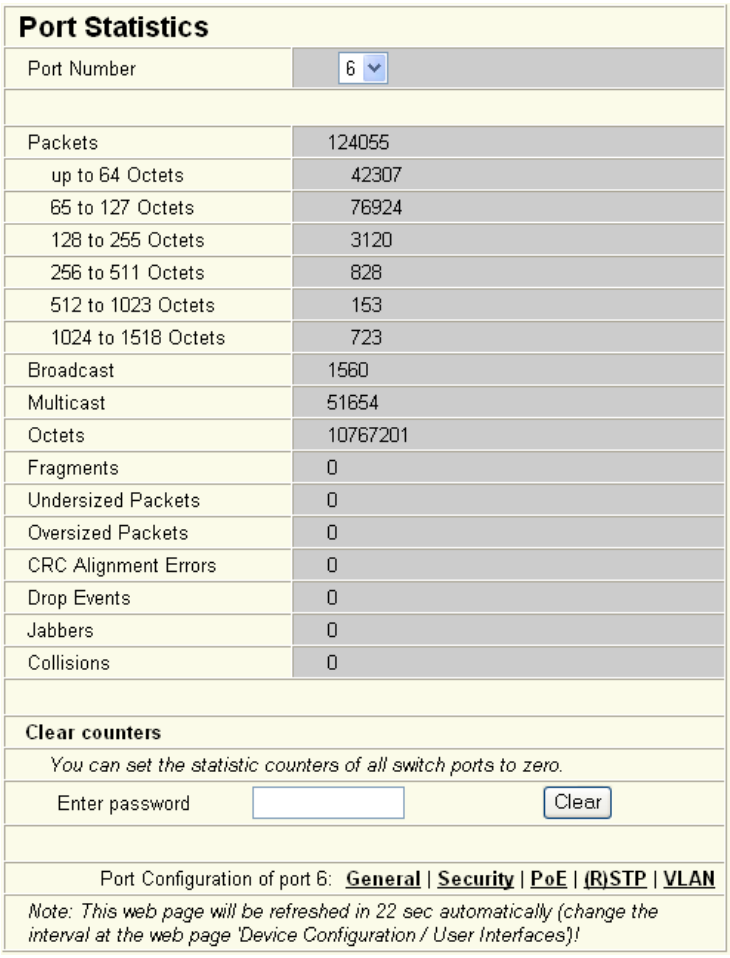


Bild 4-35 Webseite „Port Statistics“

Menü „Ports\Port POF Table“

Auf dieser Seite werden die verfügbaren Informationen zu den POF-SCRJ-Interface-Modulen angezeigt.

POF-SCRJ transceiver diagnostics Port Table

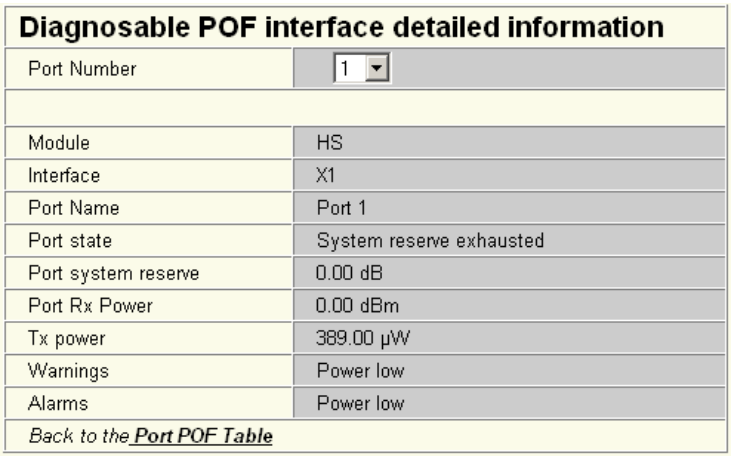
Module	Interface	Port	Transceiver status	RX system reserve
HS	X1	1 (details)	System reserve exhausted	System Reserve is 0.00 dB
		2 (details)	System reserve exhausted	System Reserve is 0.00 dB
	X2	3 (details)	System reserve exhausted	System Reserve is 0.00 dB
		4 (details)	System reserve exhausted	System Reserve is 0.00 dB
	X3	5 (details)	No diagnosable POF module plugged on this port	
		6 (details)	No diagnosable POF module plugged on this port	

Bild 4-36 Webseite „POF-SCRJ transceiver diagnostics Port Table“

Folgende Stati können unter „Transceiver status“ angezeigt werden:

– System Hardware does not support diagnoseable POF modules“ (Diese Hardware unterstützt keine POF-SCRJ-Diagnose)
– No POF-SCRJ Interface modules present (Es ist kein POF-SCRJ-Modul gesteckt)
– POF-SCRJ Interface module is present and OK (Die Systemreserve ist größer 2 dB und wird unter „RX system reserve angezeigt)
– POF-SCRJ Interface module is present, but the system reserve is low (Die Systemreserve ist kleiner 2 dB, aber größer 0 dB)
– POF-SCRJ Interface module is present, but the system reserve is exhausted (Keine Systemreserve vorhanden - die empfangene Lichtleistung liegt unterhalb des erforderlichen Mindestwertes)

Wenn Sie unterhalb der Port-Nummer auf Details klicken, finden Sie im nachfolgenden Fenster Detail-Informationen zu den Sende-/Empfangseigenschaften des jeweiligen Ports.



Diagnosable POF interface detailed information

Port Number	1
Module	HS
Interface	X1
Port Name	Port 1
Port state	System reserve exhausted
Port system reserve	0.00 dB
Port Rx Power	0.00 dBm
Tx power	389.00 µW
Warnings	Power low
Alarms	Power low

Back to the ***Port POF Table***

Bild 4-37 Webseite „Diagnose

Menü „Ports\Port Mirroring“

Aktivieren/deaktivieren und Einstellung des Port Mirroring. Port Mirroring dient dem passiven Mitlesen von Daten, die über einen ausgewählten Port gehen. Dazu wird am Destination-Port ein Messgerät (PC) angeschlossen, das die Daten aufzeichnet, aber selbst nicht aktiv werden darf.

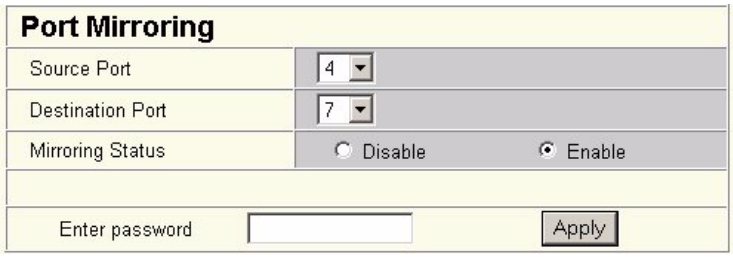


Bild 4-38 Webseite „Port Mirroring“

Falls der Source-Port einer der Ports von Port 1 bis Port 8 ist, dann sollte auch der Destination-Port einer aus der genannten Gruppe sein, um CRC-Fehler und Paketverluste zu vermeiden. Gleiches gilt für die Ports 9 bis 16 und für die Ports 17 bis 24.

Multicast-Datenpakete von angelegten Multicast-Gruppen können nicht gespiegelt werden. Um Multicast-Datenpakete auch am eingestellten Destination-Port empfangen zu können, muss der Destination-Port in die entsprechenden Multicast-Gruppen eingefügt werden.

Die Port-Auslastung wird gemäß den eingestellten Übertragungsparametern errechnet. Beispiel: Ein Source-Port wird mit 100 MBit/s betrieben und erreicht eine Auslastung von 5 %. Der Destination-Port wird mit 10 MBit/s betrieben. Daher erreicht der Destination-Port bei gleichem Datenaufkommen eine Auslastung von 50 %.

Das Einstellen gleicher Ports hat zur Folge, dass das Port-Mirroring abgeschaltet wird. Der Source-Port wird auf „0“ gesetzt.

Menü „Ports\Port Security“

Um hier je Port individuelle Einstellungen vornehmen zu können, muss zuvor auf der Seite „Switch Station\Services“ die Funktion „Port Security“ aktiviert werden. Unter „Security Mode“ wählen Sie zwischen folgenden Optionen:

– None
  Keine Sicherheitseinstellung für diesen Port.
– Trap only
  Beim Zugriff einer nicht freigegebenen MAC-Adresse auf den Port wird ein Trap an die zuvor definierten Trap-Ziele versendet. Der Port wird nicht blockiert.

Für jede MAC-Adresse, die illegal auf einen Port zugreift, wird ein Trap versendet. Greift nach Ablauf der Aging Time, wenn diese MAC-Adresse wieder aus der MAC-Adresstabelle gelöscht wurde, diese MAC-Adresse wieder auf diesen Port zu, wird erneut ein Trap versendet. Ist die Zeitspanne der illegalen Zugriffe jedoch kürzer als die Aging Time, wird nur ein Trap beim ersten Zugriff versendet.

– Block Packets
  Nach Eingang nicht autorisierter Pakete wird der Port für alle Pakete blockiert. Es wird ein Trap versendet, der auf den verbotenen Zugriffsversuch hinweist. Der Port bleibt solange blockiert, bis die Blockade vom Administrator mit Hilfe des „Unlock“-Button auf der Seite „Switch Station\Ports\Port Security“ aufgehoben wird.
– Block Packets with automatic reenabling
  Nach Eingang nicht autorisierter Pakete wird der Port für alle Pakete blockiert. Es wird ein Trap versendet, der auf den verbotenen Zugriffsversuch hinweist. Nach Ablauf der Aging Time wird der Port automatisch wieder freigegeben.

Die Funktion „Port Security“ ist ausschließlich für Ports geeignet, an denen Endgeräte angeschlossen sind. Die Verwendung bei Backbone- oder Uplink-Ports, insbesondere bei aktiviertem RSTP, wird nicht empfohlen.

Unter „Allowed MAC Address“ geben Sie die freigegebenen MAC-Adressen und einen Namen an.

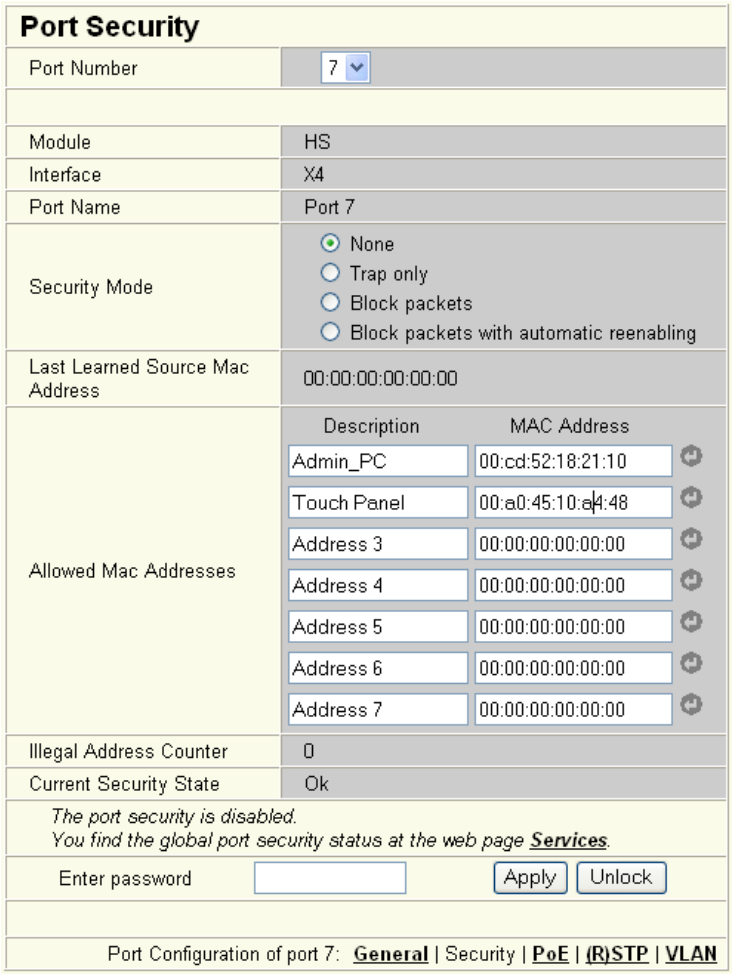


Bild 4-39 Webseite „Port Security“

Mit Hilfe des „Unlock“-Buttons kann die Port-Blockade wieder aufgehoben werden.

Unter „Last Source MAC Address“ wird die MAC-Adresse angezeigt, die zuletzt auf diesen Port zugegriffen hat. Ist der Port geblockt, finden Sie hier die MAC-Adresse, die für die Blockade verantwortlich ist.

Menü „Ports\Port PoE Table“

Dieses Menü zeigt die verfügbaren PoE-Statusinformationen je Port an.

Power over Ethernet Port Table

Module	Interface	Port	PoE fault status	PoE operational status
HS	X1	1	No PoE enabled powered device connected to this port	
		2	No fault detected	Class 3 device
	X2	3	No PoE enabled powered device connected to this port	
		4	No PoE enabled powered device connected to this port	
	X3	5	Missing 48V supply fault	
		6	Missing 48V supply fault	

Bild 4-40 Webseite „Power over Ethernet Port Table“

Folgende Stati werden unterstützt:

– Kein Fehler
– Fehler in der externen PoE-Versorgungsspannung
– Temperatur zu hoch
– Strombegrenzung aktiviert
– Load disconnected
– Der PoE-Controller reagiert nicht, evtl. fehlt die 48-V-Versorgung
– Kein PoE-Interface-Module an diesem Platz gesteckt
– Der Switch unterstützt keine PoE-Interface-Module
– Kein PoE-Verbraucher an diesem Port angeschlossen
– Port Power over Ethernet Configuration

Menü „Ports\Port Power over Ethernet Configuration“

In diesem Menü können Sie portbezogen die Konfigurationseinstellungen für Power-over-Ethernet vornehmen.

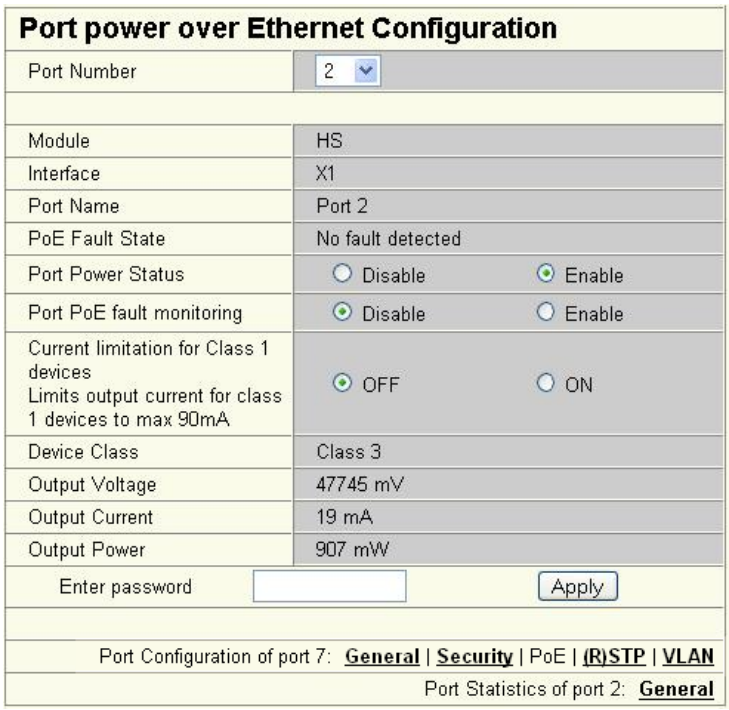
Das PoE-Interface-Modul wird ab der Firmware-Version 4.0 unterstützt. Bei einer Firmware-Version <4.0 wird das Modul wie ein Standard-RJ45-Interface-Modul behandelt. Ohne Unterstützung durch die Firmware und die Hardware (Systembus) kann das Modul im PoE-Modus ohne jedes Management betrieben werden. Es stehen dann keine Konfigurationsmöglichkeiten und keine Diagnosedaten zur Verfügung.

Der Einsatz des PoE-Interface-Moduls setzt in der Kopfstation die Systembus-Firmware 5.00 oder höher und in den Erweiterungsmodulen die Systembus-Firmware 4.00 oder höher voraus. Ist in der Kopfstation oder in irgendeinem Erweiterungsmodul diese Bedingung nicht erfüllt, so steht das PoE-Management im **gesamten** System nicht zur Verfügung. Ohne Management-Unterstützung können PoE-Interface-Module ohne jedes Management betrieben werden. Es stehen dann keine Konfigurationsmöglichkeiten und keine Diagnosedaten zur Verfügung, angeschlossene Endgeräte werden aber dennoch mit Spannung versorgt. Auf der Webseite „Device Information/General“ wird die Systembus-Firmware angezeigt.

Die PoE-Konfigurationsmöglichkeiten stehen auch dann zur Verfügung, wenn kein PoE-Interface-Modul gesteckt ist. Wird ein PoE-Interface-Modul gesteckt, so wird die Konfiguration nach einigen Sekunden auf das Modul übertragen.

Eigenschaften des PoE-Betriebs

– Es können bis zu zwölf PoE-Interface-Module mit insgesamt 24 Ports gleichzeitig am MMS betrieben werden.
– Die Konfigurationsübertragung auf das Interface-Modul ist nur bei angeschlossener 48-V-Versorgung möglich.
– Folgende Management-Funktionen stehen zur Verfügung:
  - Fehlerzustände je Port im Display anzeigen und über Alarm-Kontakt melden (ja/nein)
  - Spannung je Port ein-/ausschalten
  - Strombegrenzung für Verbraucher, die sich als Klasse 1 (Class 1) Geräte klassifiziert haben.
– Folgende Diagnose-Angaben werden angezeigt:
  - Kein Fehler
  - Überspannung/Unterspannung
  - Thermischer Fehler
  - Überlast
  - Disconnected Load (die Stromaufnahme an diesem Port beträgt weniger als 10 mA, die Versorgungsspannung wird vom PoE-Modul abgeschaltet)
  - 48-V-Versorgung fehlt
  - Kein PoE-Endgerät angeschlossen
  - Kein PoE-Interface-Modul an diesem Port erkannt
  - Fehlende Hardware-Unterstützung aufgrund des Systembusses
  - Die detektierte Klasse eines angeschlossenen Endgerätes (Class 0 bis Class 4)
  - Die Ausgangsspannung sowie den Ausgangsstrom



Port power over Ethernet Configuration

Port Number	2
Module	HS
Interface	X1
Port Name	Port 2
PoE Fault State	No fault detected
Port Power Status	○ Disable ◉ Enable
Port PoE fault monitoring	◉ Disable ○ Enable
Current limitation for Class 1 devices Limits output current for class 1 devices to max 90mA	◉ OFF ○ ON
Device Class	Class 3
Output Voltage	47745 mV
Output Current	19 mA
Output Power	907 mW
Enter password	Apply

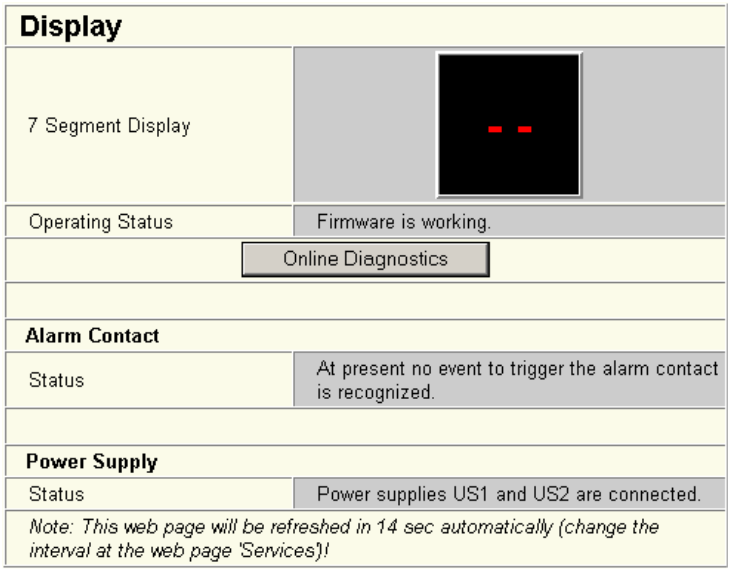
Port Configuration of port 7: General | Security | PoE | (R)STP | VLAN

Port Statistics of port 2: General

Bild 4-41 Webseite „Port power over Ethernet Configuration“

Menü „Diagnostics\Display“

Aktuelle Anzeige des 7-Segment-Displays, sowie die Stati des Meldekontakts und der redundanten Spannungsversorgung.



Display

7 Segment Display	- -
Operating Status	Firmware is working.
Online Diagnostics	
Alarm Contact	
Status	At present no event to trigger the alarm contact is recognized.
Power Supply	
Status	Power supplies US1 and US2 are connected.

Note: This web page will be refreshed in 14 sec automatically (change the interval at the web page 'Services')!

Bild 4-42 Webseite „Display“

Durch Klicken auf „Online Diagnostics“ wird die aktuelle Ansicht des Diagnose-Displays in einem kleinen Browser-Fenster dargestellt. Die Anzeige wird automatisch nach zwei Sekunden erneuert.

Menü „Diagnostics\Alarm Contact“

Hier können Sie einstellen, ob und für welche Ereignisse der Meldekontakt verwendet wird.

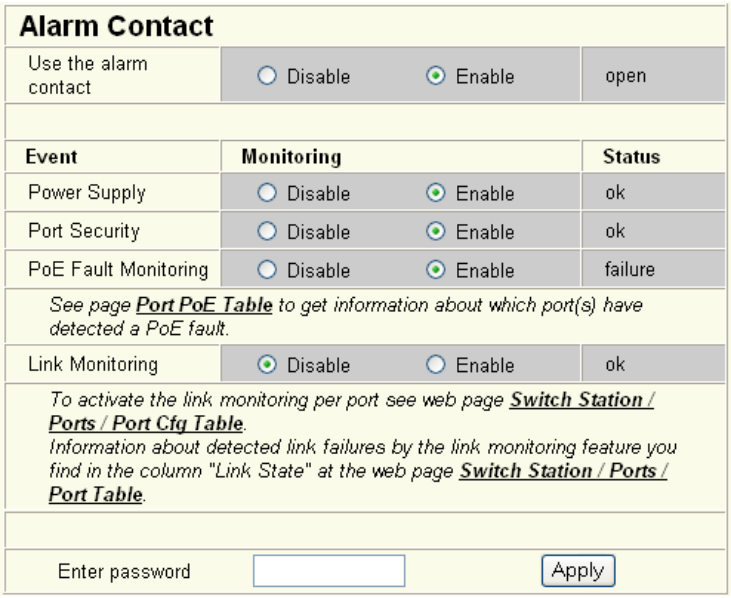


Bild 4-43 Webseite „Alarm Contact“

Durch Klicken auf den Link „Switch Station / Ports / Port Cfg Table“ (im WBM auf der Seite „Alarm Contact“) erreichen Sie die Seite zur Konfiguration der Ports.

Menü „Diagnostics\Utilization“

Hier wird die Netzauslastung jedes einzelnen Ports als Balkendiagramm angezeigt. Die Darstellung wird entsprechend des Refresh Intervalls automatisch aktualisiert.

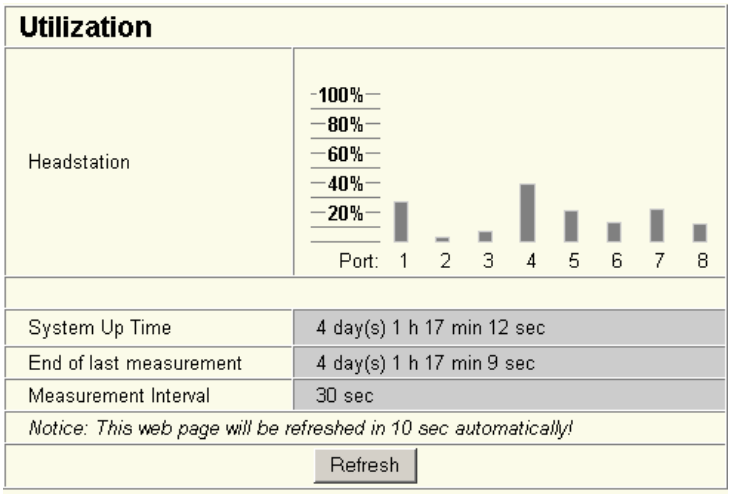


Bild 4-44 Webseite „Utilization“

Beachten Sie, dass die %-Skala in Abhängigkeit von der Auslastung gespreizt wird.

Menü „Diagnostics\Event Table“

Hier finden Sie eine Auflistung der letzten wichtigen Ereignisse. Die Liste enthält bis zu 200 Einträge, ab dem 200. Eintrag werden die ältesten Einträge überschrieben (FIFO-Prinzip - First-In-First-Out-Prnzip). Falls alte Einträge durch neue Einträge überschrieben werden, wird unterhalb des Event Tables ein entsprechender Hinweis eingeblendet.

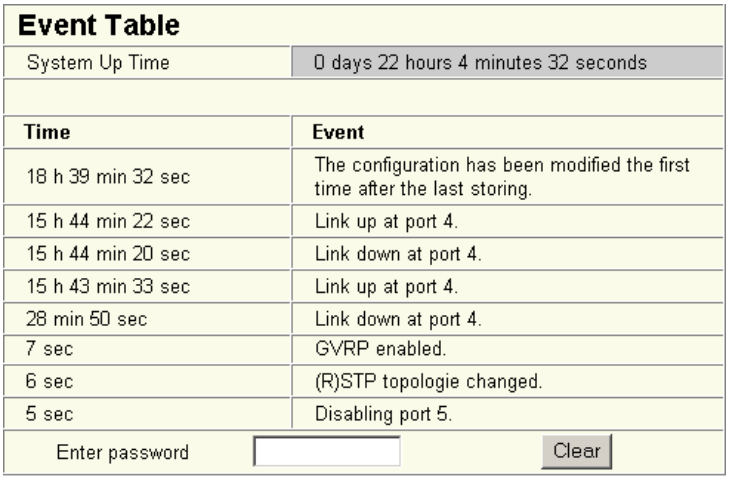

Event Table
System Up Time
0 days 22 hours 4 minutes 32 seconds
Time
Event
18 h 39 min 32 sec
The configuration has been modified the first time after the last storing.
15 h 44 min 22 sec
Link up at port 4.
15 h 44 min 20 sec
Link down at port 4.
15 h 43 min 33 sec
Link up at port 4.
28 min 50 sec
Link down at port 4.
7 sec
GVRP enabled.
6 sec
(R)STP topologie changed.
5 sec
Disabling port 5.
Enter password
Clear

Bild 4-45 Webseite „Event Table“

Mit dem „Clear“-Button können die Einträge in der Event-Table gelöscht werden.

Folgende Ereignisse werden im Event Table aufgelistet:

- Event Table cleared.
- Password has been changed.
- Password has not been changed successfully.
- Configuration has been saved.
- The configuration has been modified the first time after the last storing.
- Memory Module recognized.
- Memory Module removed.
- Memory Module cleared.
- Configuration File Transfer successfully executed.
- Configuration File Transfer was not successfully executed.
- Firmware Update was successfully executed.
- Firmware Update was not successfully executed.
- Link up at port xy.
- Link down at port xy.
- Enabling port xy.
- Disabling port xy.
- Unpermitted mac address at port xy.
- RSTP enabled.
- RSTP disabled.
- RSTP topologie changed.
- RSTP elected this switch as new root.
- IGMP Snooping enabled.
- IGMP Snooping disabled.
- IGMP Querier enabled.
- IGMP Querier disabled.
- Better query received.
- Better query received in vlan xy.
- Become active querier.
- Become active querier in vlan xy.
- GVRP enabled.
- GVRP disabled.
- Power Supply US1 lost.
- Power Supply US2 lost.
- Power Supply US1 and US2 are connected now.
- LLDP Agent enabled.
- LLDP Agent disabled.
- LLDP recognized new neighbor at port xy.
- LLDP neighborhood information changed at port xy.
- LLDP neighbor information become obsolete at port xy.
- Power over Ethernet fault detected at least one port.
- No Power over Ethernet faults detected any more.
- One of the interface modules is not supported by the system hardware. The interface will be able to send or receive data but can not be diagnosed.
- A Profinet connection was established.
- The Profinet connection was terminated.
- Diagnosable POF module: OK on port xy.

– Diagnosable POF module: Warning level reached on port xy.
– Diagnosable POF module: Critical status on port xy.
– Configuration difference detected.
– Configuration difference detected at slot.
– Configuration difference removed.
– MRP Client activated.
– MRP Manager activated.
– MRP disabled.
– MRP Manager detects a loop failure.
– MRP Manager detects a closed loop.

Menü „Diagnostics\Mac Address Table“

Hier finden Sie eine Auflistung, welche MAC-Adresse an welchem Switch-Port erkannt wurde und welche VLAN-ID sie trägt. Falls an einem Port für einen Zeitraum, der länger andauert als die Aging Time, kein Paket empfangen wird, wird der Eintrag gelöscht.

Über Download ist ein Export als Excel-Tabelle möglich. Hiermit steht eine effiziente Analyse-Möglichkeit zur Verfügung, die sich insbesondere in größeren Netzwerken als hilfreich erweist.

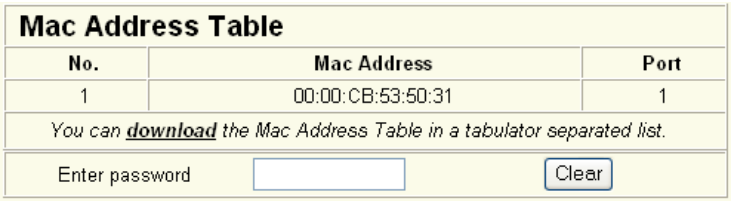


Bild 4-46 Webseite „Mac Address Table“

Mit dem „Clear“-Button können die Einträge der Mac Address Table gelöscht werden.

Menü „Diagnostics\LLDP“

Erläuterungen zu LLDP finden Sie im Kapitel „LLDP - Link Layer Discovery Protocol“ auf Seite 10-1.

4.2.3.5 (Rapid) Spanning Tree / MRP / Multicast Filtering / VLAN

Erläuterungen zu (Rapid) Spanning Tree finden Sie im Kapitel 5 „(Rapid) Spanning Tree“.

Erläuterungen zum Medien-Redundanz-Protokoll (MRP) finden Sie im Kapitel 6 „Medien-Redundanz-Protokoll - MRP“.

Zu Multicast Filtering finden Sie die Erklärungen im Kapitel 7 „Multicast Filtering“.

Erläuterungen zur VLAN-Funktion finden Sie im Kapitel 8 „Virtual Local Area Network - VLAN“.

4.3 Simple Network Management Protocol - SNMP

4.3.1 Allgemeine Funktion

SNMP ist ein herstellerneutraler Standard für das Ethernet-Management. Er definiert Kommandos zum Lesen und Schreiben von Informationen und definiert Formate von Fehler- und Status-Meldungen. Außerdem bietet SNMP ein strukturiertes Modell, das aus Agenten mit ihrer jeweiligen MIB (Management Informationen Base) und einem Manager besteht. Der Manager ist eine Software, die auf einer Netzmanagement-Station ausgeführt wird. Die Agenten befinden sich innerhalb von Switches, Busklemmen, Routern und anderen Geräten, die SNMP unterstützen. Die Aufgabe der Agenten ist das Sammeln und das Bereitstellen von Daten in der MIB. Der Manager fordert diese Informationen regelmäßig an und stellt sie dar. Mit Daten vom Manager in die MIB geschrieben, ist eine Konfiguration der Geräte möglich. In dringenden Fällen können die Agenten auch Meldungen (Traps) direkt an den Manager schicken.

Alle Konfigurations-Änderungen, die nach einem Neustarts des MMS wirksam sein sollen, müssen mit Hilfe des Objekts „flWorkFWCtrlConfSave“ dauerhaft gespeichert werden.

SNMP-Interface

Die managebaren Komponenten der Produktreihe Factory Line verfügen jeweils über einen SNMP-Agenten. Dieser Agent eines FL SWITCH MM HS verwaltet die Management Information Base II (MIB 2) nach RFC1213, RMON-MIB, Bridge-MIB, If-MIB, Etherlike-MIB, Iana-address-family-MIB, IANAifType-MIB, SNMPv2-MIB, SNMP-FRAMEWORK-MIB, P-Bridge-MIB, Q-Bridge-MIB, RSTP-MIB, LLDP-MIB, pnoRedundancy-MIB und die privaten SNMP-Objekte von Phoenix Contact (FL-SWITCH-M-MIB).

Über das Simple Network Management Protocol erhalten Netzwerk Management-Stationen, wie zum Beispiel ein PC mit dem Factory Manager, die Möglichkeit, Konfigurations- und Diagnose-Daten der Netzwerkteilnehmer auszulesen und zu verändern. Es ist auch möglich, beliebige SNMP-Tools oder Netzwerk-Management-Tools für den Zugriff über SNMP auf Factory Line-Produkte zu nutzen. Dazu sind die von dem jeweiligen Gerät unterstützen MIBs den SNMP-Management-Tools zur Verfügung zu stellen.

Zum einen sind dies weltweit gültige MIBs, die in RFCs (Request for comments) festgelegt und beschrieben sind. Dazu zählt zum Beispiel die MIB2 nach RFC1213, die von jedem SNMP-fähigen Netzwerkteilnehmer unterstützt wird. Zum anderen kann jeder Hersteller eigene private SNMP-Objekte festlegen, die dann in dem großen SNMP-Objekt-Baum in einem privaten Herstellerbereich eingeordnet werden. Für diesen privaten (enterprise) Bereich ist dann jeder Hersteller selber verantwortlich, d. h., dass einer Objekt-ID zum Beispiel nur einmalig ein Objekt zugewiesen (Objektname und Parameter) und veröffentlicht werden darf. Wird dieses Objekt danach nicht mehr benötigt, so wird es als auslaufend gekennzeichnet, aber unter keinen Umständen zum Beispiel mit anderen Parametern erneut verwendet.

Die ASN1-SNMP-Objekte werden von Phoenix Contact durch die Veröffentlichung der Beschreibung auf den Internet-Seiten bekannt gegeben.

Das Lesen der SNMP-Objekte ist nicht durch ein Passwort geschützt. Es muss zwar im SNMP beim lesenden Zugriff ein Passwort angegeben werden, dieses ist aber, wie bei Netzwerkteilnehmern üblich, auf „public“ eingestellt und kann nicht verändert werden. Das Passwort für den Schreibzugriff ist im Auslieferungszustand „private“ und kann vom Benutzer verändert werden.

SNMP, Web-Interface, Telnet und serielles Terminal verwenden dasselbe durch den Anwender veränderbare Passwort.

Ein weiterer Nutzen für den Anwender bietet das Simple Network Management durch die Möglichkeit zur Versendung von Traps.

Management Information Base (MIB)

Datenbank, in die alle Daten (Objekte und Variablen) eingetragen werden, die zum Netzwerkmanagement benötigt werden.

Agent

Ein Agent ist eine Software, die Daten des Netzwerkteilnehmers, auf dem sie installiert ist, sammelt und auf Anforderung versendet. Die Agents residieren in allen managebaren Komponenten eines Netzwerks und übertragen die Werte spezieller Einstellungen und Parameter zu der Management-Station. Nach Aufforderung eines Managers oder beim Auftreten eines Ereignisses übermittelt der Agent die zuvor gesammelten Informationen zu der Management-Station.

Traps

Traps sind spontane SNMP-Alarm- oder Informationsmeldungen, die ein SNMP-fähiges Gerät von sich aus auf besondere Ereignisse hin versendet. Die Traps werden mit höchster Priorität ggfs. an unterschiedliche Adressen übertragen und können anschließend im Klartext von der Management-Station dargestellt werden. Die Empfänger-IP-Adressen (Trap-Targets/Receiver) dieser Traps müssen vom Anwender auf dem jeweiligen Gerät eingestellt werden.

trapPasswdAccess

OID	1.3.6.1.4.1.4346.11.11.3.0.1
Beschreibung	Wird bei jeder Änderung oder jedem Änderungsversuch auf das Geräte-Passwort an die definierten Trap-Receiver gesendet und enthält eine Information zum Status der letzten Änderung oder des letzten Änderungsversuchs.

trapFWHealth

OID	1.3.6.1.4.1.4346.11.11.3.0.2
Beschreibung	Wird bei jeder Firmware-relevanten Änderung des Diagnose-Displays gesendet und enthält weitere Informationen zum Firmware-Status.

trapFWConf

OID	1.3.6.1.4.1.4346.11.11.3.0.3
Beschreibung	Wird bei jedem Speichern der Konfiguration gesendet und informiert so die Management-Station über die erfolgreiche Konfigurationsspeicherung. Dieser Trap wird bei Konfigurationsänderungen (Port-Name, Port-Modus, Gerätename, IP-Adresse, Trap-Receiver-Adresse, Port-Mirroring o.ä.), die noch nicht dauerhaft gespeichert sind, verschickt. Der Trap stellt somit eine Warnung dar, dass die Änderungen (ohne eine dauerhafte Speicherung) nach einem Reset verloren sind.

trapPowerSupply

OID	1.3.6.1.4.1.4346.11.11.3.0.4
Beschreibung	Wird bei jedem Ausfall der redundanten Spannungseinspeisung gesendet.

trapSecurityPort

OID	1.3.6.1.4.1.4346.11.11.3.0.5
Beschreibung	Wird bei jedem Zugriff einer nicht freigegebenen MAC-Adresse auf einen Port versendet.

trapRstpRingFailure

OID	1.3.6.1.4.1.4346.11.11.3.0.6
Beschreibung	Wird bei einer Link-Unterbrechung im redundanten RSTP-Ring versendet.

trapPofDiagPort

OID	1.3.6.1.4.1.4346.11.11.3.0.7
Beschreibung	Wird bei jeder Statusänderung des POF-SCRJ-Ports versendet.

trapPoEPort

OID	1.3.6.1.4.1.4346.11.11.3.0.8
Beschreibung	Wird bei jeder Statusänderung des PoE-Ports versendet.

trapMrpStatusChange

OID	1.3.6.1.4.1.4346.11.11.3.0.9
Beschreibung	Nur bei MRP-Manager: Wird bei jeder Statusänderung eines MRP-Ring-Ports versendet.

trapManagerConnection

OID	1.3.6.1.4.1.4346.11.11.3.0.99
Beschreibung	Trap zum Testen der Verbindung zwischen SNMP Agent und der Netzwerk-Management-Station.

4.3.2 Schematische Darstellung von SNMP-Management

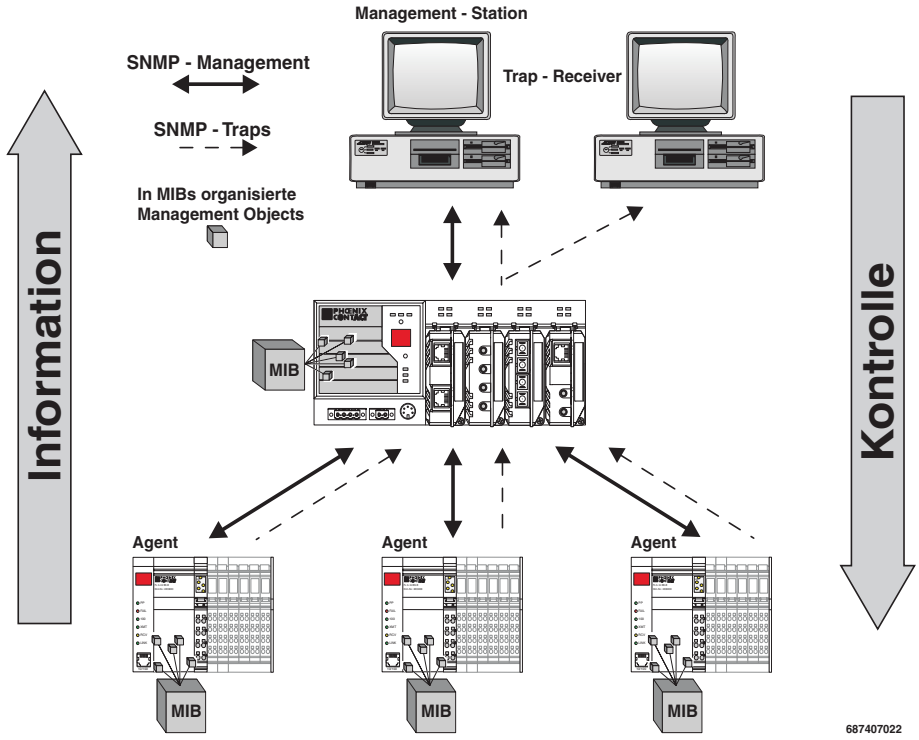


Bild 4-47 Schematische Darstellung von SNMP

4.3.2.1 Baumstruktur der MIB

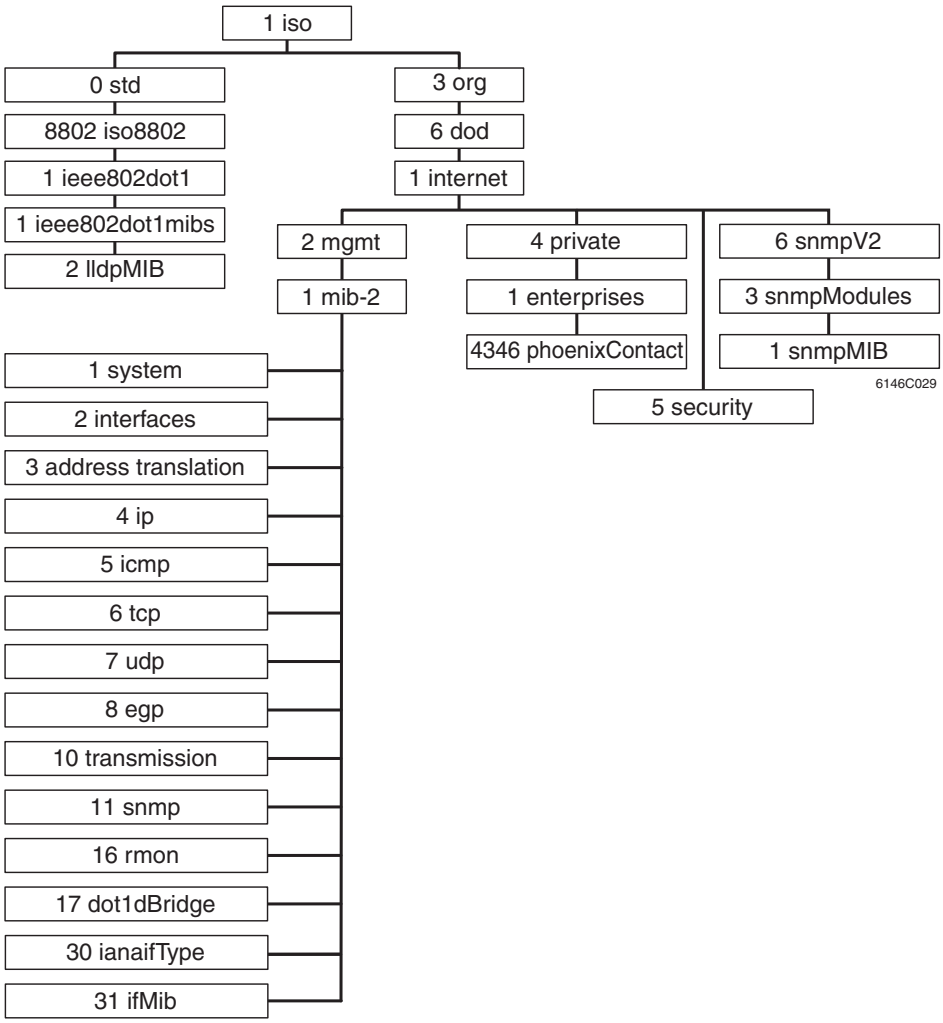


Bild 4-48 Baumstruktur der MIB

Nicht alle Geräte unterstützen alle Objektklassen. Die Abfrage einer nicht unterstützten Objektklasse liefert den Wert „not supported“. Der Versuch, eine nicht unterstützte Objektklasse zu ändern, hat die Meldung „badValue“ zur Folge.

4.3.3 RFC1213-MIB - MIB II

4.3.3.1 System-Gruppe (1.3.6.1.2.1.1)

Die System-Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält systembezogene Objekte. Hat ein Agent keinen Wert für eine Variable, dann wird mit einem String der Länge 0 geantwortet.

(1) system

– (1) sysDescr
– (2) sysObjectID
– (3) sysUpTime
– (4) sysContact
– (5) sysName
– (6) sysLocation
– (7) sysServices
– (8) sysORLastChange
– (9) sysORTable

sysDescr

OID	1.3.6.1.2.1.1.1.0
Syntax	Octet String (Größe: 0-255)
Zugriff	lesen
Beschreibung	Eine verbale Beschreibung des Eintrags. Dieser Wert sollte den vollen Namen und Versionsnummer von - Typ der System-Hardware - Operationssystem-Software und - Netzwerk-Software enthalten. Die Beschreibung darf nur aus druckbaren ASCII-Zeichen bestehen.

sysObjectID

OID	1.3.6.1.2.1.1.2.0
Syntax	Objekt-Identifizierer
Zugriff	lesen
Beschreibung	Die Autorisierungs-Identifikation des Herstellers des Netzwerk-Management-Subsystems, welches in diesem Gerät integriert ist. Dieser Wert ist innerhalb des SMI enterprices subtree (1.3.6.1.4.1) platziert und beschreibt welche Art von Gerät verwaltet wird. Zum Beispiel: wenn dem Hersteller „Phoenix Contact GmbH“ der subtree 1.3.6.1.4.1.4346 zugewiesen ist, dann kann er seiner Brücke den Identifizierer 1.3.6.1.4.1.4346.2.1 zuordnen.

sysUpTime

OID	1.3.6.1.2.1.1.3.0
Syntax	TimeTicks
Zugriff	lesen
Beschreibung	Die Zeit in hundertstel Sekunden seit dem letzten Zurücksetzen der Netzwerk-Management-Einheit.

sysContact

OID	1.3.6.1.2.1.1.4.0
Syntax	Octet String (Größe: 0-255)
Zugriff	lesen und schreiben
Beschreibung	Die verbale Identifikation der Kontaktperson für diesen verwalteten Knoten zusammen mit einer Information, wie diese Person erreichbar ist.

sysName

OID	1.3.6.1.2.1.1.5.0
Syntax	Octet String (Größe: 0-255)
Zugriff	lesen und schreiben
Beschreibung	Ein für die Administration bezeichnender Namen für diesen Knoten. Vereinbarungsgemäß ist dies der voll qualifizierende Name in der Domäne.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	Octet String (Größe: 0-255)
Zugriff	lesen und schreiben
Beschreibung	Der physikalische Ort, an dem sich dieser Knoten befindet (z. B. "Halle1, 3. OG").

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0-127)
Zugriff	lesen
Beschreibung	Bezeichnet eine Menge von Diensten, welche dieses Gerät anbietet. Der Wert ist eine Summe aus mehreren Summanden. Für jeden Layer des OSI Referenzmodells gibt es einen Summanden in der Form (2^{L-1}), wobei L den Layer bezeichnet. Z. B.: Für einen Knoten, der in erster Linie Routing-Funktionen ausführt, ist der Wert (2^{3-1}) = 4. Für einen Knoten, der ein Host ist, welcher Applikationsdienste anbietet, ist der Wert (2^{4-1}) + (2^{7-1}) = 72.

sysORLastChange

OID	1.3.6.1.2.1.1.8
Syntax	Timeticks
Zugriff	lesen
Beschreibung	Nennt den Wert der SysUp-Time bei der letzten Systemänderung.

sysORTable

OID	1.3.6.1.2.1.1.9
Syntax	Timeticks
Zugriff	lesen
Beschreibung	Diese Tabelle enthält die Objekte: sysORIndex, sysORID, sysORDescr und sysORUp-Time.

4.3.3.2 Interface-Gruppe (1.3.6.1.2.1.2)

Die Interface-Gruppe enthält Informationen über die Geräteschnittstellen.

(2) interfaces
-- (1) ifNumber
-- (2) ifTable
-- (1) if Entry
-- (1) ifIndex
-- (2) ifDescr
-- (3) ifType
-- (4) ifMtu
-- (5) ifSpeed
-- (6) ifPhysAddress
-- (7) ifAdminStatus
-- (8) ifOperStatus
-- (9) ifLastChange
-- (10) ifInOctets
-- (11) ifInUcastPkts
-- (12) ifInNUcastPkts
-- (13) ifInDiscards
-- (14) ifInErrors
-- (15) ifInUnknownProtos
-- (16) ifOutOctets
-- (17) ifOutUcastPkts
-- (18) ifOutNUcastPkts
-- (19) ifOutDiscards
-- (20) ifOutErrors
-- (21) ifOutQLen
-- (22) ifSpecific

4.3.3.3 Address-Translation-Gruppe (1.3.6.1.2.1.3)

Die Address-Translation-Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält Informationen über die Adressenzuordnung.

(3) at
-- (1) atTable
-- (1) atEntry
-- (1) atIfIndex
-- (2) atPhysAddress
-- (3) atNetAddress

4.3.3.4 Internet-Protocol-Gruppe (1.3.6.1.2.1.4)

Die Internet-Protocol-Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält Informationen, die die IP-Vermittlung betreffen.

(4) ip
- -- (1) ipForwarding
- -- (2) ipDefaultTTL
- -- (3) ipInReceives
- -- (4) ipInHdrErrors
- -- (5) ipInAddrErrors
- -- (6) ipForwDatagrams
- -- (7) ipInUnknownProtos
- -- (8) ipInDiscards
- -- (9) ipInDelivers
- -- (10) ipOutRequests
- -- (11) ipOutDiscards
- -- (12) ipOutNoRoutes
- -- (13) ipReasmTimeout
- -- (14) ipReasmReqds
- -- (15) ipReasmOKs
- -- (16) ipReasmFails
- -- (17) ipFragOKs
- -- (18) ipFragFails
- -- (19) ipFragCreates
- -- (20) ipAddrTable
  - -- (1) ipAddrEntry
    - -- (1) ipAdEntAddr
    - -- (2) ipAdEntIfIndex
    - -- (3) ipAdEntNetMask
    - -- (4) ipAdEntBcastAddr
    - -- (5) ipAdEntReasmMaxSize
- -- (21) ipRouteTable
  - -- (1) ipRouteEntry
    - -- (1) ipRouteDest
    - -- (2) ipRouteIfIndex
    - -- (3) ipRouteMetric1
    - -- (4) ipRouteMetric2
    - -- (5) ipRouteMetric3
    - -- (6) ipRouteMetric4
    - -- (7) ipRouteNextHop
    - -- (8) ipRouteType
    - -- (9) ipRouteProto
    - -- (10) ipRouteAge
    - -- (11) ipRouteMask
    - -- (12) ipRouteMetric5
    - -- (13) ipRouteInfo
- -- (22) ipNetToMediaTable
  - -- (1) ipNetToMediaEntry

-- (1) ipNetToMediaIfIndex
-- (2) ipNetToMediaPhysAddress
-- (3) ipNetToMediaNetAddress
-- (4) ipNetToMediaType
-- (23) ipRoutingDiscards

4.3.3.5 ICMP-Gruppe (1.3.6.1.2.1.5)

Die Internet Control Message Protocol Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält Informationen zur Fehlerbehandlung und Steuerung im Internet-Datenverkehr.

(5) icmp
-- (1) icmpInMsgs
-- (2) icmpInErrors
-- (3) icmpInDestUnreachs
-- (4) icmpInTimeExcds
-- (5) icmpInParmProbs
-- (6) icmpInSrcQuenchs
-- (7) icmpInRedirects
-- (8) icmpInEchos
-- (9) icmpInEchoReps
-- (10) icmpInTimestamps
-- (11) icmpInTimestampReps
-- (12) icmpInAddrMasks
-- (13) icmpInAddrMaskReps
-- (14) icmpOutMsgs
-- (15) icmpOutErrors
-- (16) icmpOutDestUnreachs
-- (17) icmpOutTimeExcds
-- (18) icmpOutParmProbs
-- (19) icmpOutSrcQuenchs
-- (20) icmpOutRedirects
-- (21) icmpOutEchos
-- (22) icmpOutEchoReps
-- (23) icmpOutTimestamps
-- (24) icmpOutTimestampReps
-- (25) icmpOutAddrMasks
-- (26) icmpOutAddrMaskReps

4.3.3.6 Transfer-Control-Protocol-Gruppe (1.3.6.1.2.1.6)

Die Transfer-Control-Protocol-Gruppe hat für alle Systeme mit implementiertem TCP Pflichtcharakter. Instanzen von Objekten, die Informationen über eine bestimmte TCP-Verbindung beschreiben, haben nur solange Bestand, wie die Verbindung besteht.

(6) tcp
- -- (1) tcpRtoAlgorithm
- -- (2) tcpRtoMin
- -- (3) tcpRtoMax
- -- (4) tcpMaxConn
- -- (5) tcpActiveOpens
- -- (6) tcpPassiveOpens
- -- (7) tcpAttemptFails
- -- (8) tcpEstabResets
- -- (9) tcpCurrEstab
- -- (10) tcpInSegs
- -- (11) tcpOutSegs
- -- (12) tcpRetransSegs
- -- (13) tcpConnTable
  - -- (1) tcpConnEntry
    - -- (1) tcpConnState
    - -- (2) tcpConnLocalAddress
    - -- (3) tcpConnLocalPort
    - -- (4) tcpConnRemAddress
    - -- (5) tcpConnRemPort
- -- (14) tcpInErrs
- -- (15) tcpOutRsts

4.3.3.7 User-Datagram-Protocol-Gruppe (1.3.6.1.2.1.7)

Die User-Datagram-Protocol-Gruppe hat für alle Systeme mit implementiertem UDP Pflichtcharakter.

(7) udp
- -- (1) udpInDatagrams
- -- (2) udpNoPorts
- -- (3) udpInErrors
- -- (4) udpOutDatagrams
- -- (5) udpTable
  - -- (1) udpEntry
    - -- (1) udpLocalAddress
    - -- (2) udpLocalPort

4.3.3.8 egp-Gruppe (1.3.6.1.2.1.8)

(8) egp
-- (1) egpInMsgs
-- (2) egpInErrors
-- (3) egpOutMsgs
-- (4) egpOutErrors
-- (5) egpNeighTable
-- (1) egpNeighEntry
-- (1) egpNeighState
-- (2) egpNeighAddr
-- (3) egpNeighAs
-- (4) egpNeighInMsgs
-- (5) egpNeighInErrs
-- (6) egpNeighOutMsgs
-- (7) egpNeighOutErrs
-- (8) egpNeighInErrMsgs
-- (9) egpNeighOutErrMsgs
-- (10) egpNeighStateUps
-- (11) egpNeighStateDowns
-- (12) egpNeighIntervalHello
-- (13) egpNeighIntervallPoll
-- (14) egpNeighMode
-- (15) egpNeighEventTrigger
-- (6) egpAs

4.3.3.9 Transmission-Gruppe (1.3.6.1.2.1.10)

(10) transmission

4.3.3.10 Simple-Network-Management-Protocol-Gruppe (1.3.6.1.2.1.11)

Die Simple-Network-Management-Protocol-Gruppe hat für alle Systeme Pflichtcharakter. In SNMP-Einrichtungen, welche optimiert sind, entweder nur einen Agenten oder nur eine Managementstation zu unterstützen, werden einige der aufgeführten Objekte mit dem Wert „0“ beschrieben sein.

(11) snmp
-- (1) snmpInPkts
-- (2) snmpOutPkts
-- (3) snmpInBadVersions
-- (4) snmpInBadCommunityName
-- (5) snmpInBadCommunityUses
-- (6) snmpInASNParseErrs
-- (8) snmpInTooBigs
-- (9) snmpInNoSuchNames
-- (10) snmpInBadValues
-- (11) snmpInReadOnlys
-- (12) snmpInGenErrs
-- (13) snmpInTotalReqVars
-- (14) snmpInTotalSetVars
-- (15) snmpInGetRequests

-- (16) snmpInGetNexts
-- (17) snmpInSetRequests
-- (18) snmpInGetResponses
-- (19) snmpInTraps
-- (20) snmpOutTooBigs
-- (21) snmpOutNoSuchNames
-- (22) snmpOutBadValues
-- (24) snmpOutGenErrs
-- (25) snmpOutGetRequests
-- (26) snmpOutGetNexts
-- (27) snmpOutSetRequests
-- (28) snmpOutGetResponses
-- (29) snmpOutTraps
-- (30) snmpEnableAuthenTraps
-- (31) snmpSilentDrops
-- (32) snmpProxyDrops

4.3.4 RMON-MIB (1.3.6.1.2.1.16)

Dieser Teil der MIB liefert dem Netzmanagement ständig aktuelle und historische Daten der Netzkomponenten. Die Konfiguration von Alarmen und Ereignissen steuert die Auswertung von Zählern der Netzkomponenten. Das Ergebnis der Auswertung teilen die Agenten in Abhängigkeit von der Konfiguration mittels Traps der Managementstation mit. Folgende Gruppen werden unterstützt:

– statistics,
– history,
– alarm,
– hosts,
– hostTopN,
– matrix,
– filter,
– capture und event.

4.3.4.1 statistics (1.3.6.1.2.1.16.1)

In dieser MIB-Gruppe finden Sie Informationen über z. B. Anzahl von Unicast-, Multicast- oder Broadcast-Telegrammen, Telegrammrate und -verteilung oder Anzahl nach Fehlerart geordneter defekter Telegramme.

Die statistics-Gruppe enthält Informationen zur Netzwerklast und -qualität.

(1) etherStatsTable
-- (1) etherStatsEntry
-- (1) etherStatsIndex
-- (2) etherStatsDataSource
-- (3) etherStatsDropEvents
-- (4) etherStatsOctets
-- (5) etherStatsPkts
-- (6) etherStatsBroadcastPkts
-- (7) etherStatsMulticastPkts
-- (8) etherStatsCRCAlignErrors
-- (9) etherStatsUndersizePkts
-- (10) etherStatsOversizePkts
-- (11) etherStatsFragments
-- (12) etherStatsJabbers
-- (13) etherStatsCollisions
-- (14) etherStatsPkts64Octets
-- (15) etherStatsPkts65to127Octets
-- (16) etherStatsPkts128to255Octets
-- (17) etherStatsPkts256to511Octets
-- (18) etherStatsPkts512to1023Octets
-- (19) etherStatsPkts1024to1518Octets
-- (20) etherStatsOwner
-- (21) etherStatsStatus

4.3.4.2 history (1.3.6.1.2.1.16.2)

Die history-Gruppe enthält Statistikinformationen, die Sie auslesen und z. B. als zeitlichen Verlauf darstellen können.

(1) historyControlTable
-- (1) historyControlEntry
-- (1) historyControlIndex
-- (2) historyControlDataSource
-- (3) historyControlBucketsRequested
-- (4) historyControlBucketsGranted
-- (5) historyControlInterval
-- (6) historyControlOwner
-- (7) historyControlStatus
(2) etherhistoryTable
-- (1) etherhistoryEntry
-- (1) etherHistoryIndex
-- (2) etherHistorySampleIndex
-- (3) etherHistoryIntervalStart
-- (4) etherHistoryDropEvents
-- (5) etherHistoryOctets

-- (6) etherHistoryPkts
-- (7) etherHistoryBroadcastPkts
-- (8) etherHistoryMulticastPkts
-- (9) etherHistoryCRCAlignErrors
-- (10) etherHistoryUndersizePkts
-- (11) etherHistoryOversizePkts
-- (12) etherHistoryFragments
-- (13) etherHistoryJabbers
-- (14) etherHistoryCollisions
-- (15) etherHistoryUtilization

4.3.4.3 alarm (1.3.6.1.2.1.16.3)

Die alarm-Gruppe fragt Statistikwerte ab und vergleicht sie mit definierten Grenzwerten. Wird der Grenzwert über- oder unterschritten, wird ein Alarm und ein Trap erzeugt.

(1) alarmTable
-- (1) alarmEntry
-- (1) alarmIndex
-- (2) alarmInterval
-- (3) alarmVariable
-- (4) alarmSampleType
-- (5) alarmValue
-- (6) alarmStartupAlarm
-- (7) alarmRisingThreshold
-- (8) alarmFallingThreshold
-- (9) alarmRisingEventIndex
-- (10) alarmFallingEventIndex
-- (11) alarmOwner
-- (12) alarmStatus

4.3.4.4 hosts (1.3.6.1.2.1.16.4)

(1) hostControlTable
-- (1) hostControlEntry
-- (1) hostControlIndex
-- (2) hostControlDataSource
-- (3) hostControlTableSize
-- (4) hostControlLastDeleteTime
-- (5) hostControlOwner
-- (6) hostControlStatus
-- (2) hostTable
-- (1) hostEntry
-- (1) hostAddress
-- (2) hostCreationOrder
-- (3) hostIndex
-- (4) hostInPkts
-- (5) hostOutPkts
-- (6) hostInOctets
-- (7) hostOutOctets
-- (8) hostOutErrors

-- (9) hostOutBroadcastPkts
-- (10) hostOutMulticastPkts
-- (3) hostTimeTable
-- (1) hostTimeEntry
-- (1) hostTimeAddress
-- (2) hostTimeCreationOrder
-- (3) hostTimeIndex
-- (4) hostTimeInPkts
-- (5) hostTimeOutPkts
-- (6) hostTimeInOctets
-- (7) hostTimeOutOctets
-- (8) hostTimeOutErrors
-- (9) hostTimeOutBroadcastPkts
-- (10) hostTimeOutMulticastPkts

4.3.4.5 hostTopN (1.3.6.1.2.1.16.5)

(1) hostTopNControlTable
-- (1) hostTopNControlEntry
-- (1) hostTopNControlIndex
-- (2) hostTopNHostINdex
-- (3) hostTopNRateBase
-- (4) hostTopNTimeRemaining
-- (5) hostTopNDuration
-- (6) hostTopNRequestedSize
-- (7) hostTopNGrantedSize
-- (8) hostTopNStartTime
-- (9) hostTopNOwner
-- (10) hostTopNStatus
-- (2) hostTopNTable
-- (1) hostTopNEntry
-- (1) hostTopNReport
-- (2) hostTopNIndex
-- (3) hostTopNAddress
-- (4) hostTopNRate

4.3.4.6 matrix (1.3.6.1.2.1.16.6)

-- (1) martrixControlTable
-- (1) matrixControlEntry
-- (1) matrixControlIndex
-- (2) matrixControlDataSource
-- (3) matrixControlTableSize
-- (4) matrixControlLastDeleteTime
-- (5) matrixControlOwner
-- (6) matrixControlStatus
-- (2) matrixSDTable
-- (1) matrixSDEntry
-- (1) matrixSDSourceAddress
-- (2) matrixSDDestAddress

-- (3) matrixSDIndex
-- (4) matrixSDPkts
-- (5) matrixSDOctets
-- (6) matrixSDErrors
-- (3) matrixDSTable
-- (1) matrixDSEntry
-- (1) matrixDSSourceAddress
-- (2) matrixDSDestAddress
-- (3) matrixDSIndex
-- (4) matrixDSPkts
-- (5) matrixDSOctets
-- (6) matrixDSErrors

4.3.4.7 filter (1.3.6.1.2.1.16.7)

(1) filterTable
-- (1) filterEntry
-- (1) filterIndex
-- (2) filterChannelIndex
-- (3) filterPktDataOffset
-- (4) filterPktData
-- (5) filterPktDataMask
-- (6) filterPktDataNotMask
-- (7) filterPktStatus
-- (8) filterPktStatusMask
-- (9) filterPktStatusNotMask
-- (10) filterOwner
-- (11) filterStatus
(2) channelTable
-- (1) channelEntry
-- (1) channelIndex
-- (2) channelIfIndex
-- (3) channelAcceptTime
-- (4) channelDataControl
-- (5) channelTurnOnEventIndex
-- (6) channelTurnOffEventIndex
-- (7) channelEventIndex
-- (8) channelEventStatus
-- (9) channelMatches
-- (10) channelDescription
-- (11) channelOwner
-- (12) channelStatus

4.3.4.8 capture (1.3.6.1.2.1.16.8)

(1) bufferControlTable
-- (1) bufferControlEntry
-- (1) bufferControlIndex
-- (2) bufferControlChannelIndex
-- (3) bufferControlFullStatus
-- (4) bufferControlFullAction
-- (5) bufferControlCaptureSliceSize
-- (6) bufferControlDownloadSliceSize
-- (7) bufferControlDownloadOffset
-- (8) bufferControlMaxOctetsRequested
-- (9) bufferControlMaxOctetsGranted
-- (10) bufferControlCapturedPackets
-- (11) bufferControlTurnOnTime
-- (12) bufferControlOwner
-- (13) bufferControlStatus
(2) captureBufferTable
-- (1)captureBufferEntry
-- (1)captureBufferControlIndex
-- (2)captureBufferIndex
-- (3) captureBufferPacketID
-- (4) captureBufferPacketData
-- (5) captureBufferPacketLength
-- (6) captureBufferPacketTime
-- (7) captureBufferPacketStatus

4.3.4.9 event (1.3.6.1.2.1.16.9)

Die event-Gruppe steuert die Erzeugung der Traps beim Auftreten der zuvor beschriebenen Alarme.

(1) eventTable
-- (1) eventEntry
-- (1) eventIndex
-- (2) eventDescription
-- (3) eventType
-- (4) eventCommunity
-- (5) eventLastTimeSent
-- (6) eventOwner
-- (7) eventStatus
(2) logTable
-- (1) logEntry
-- (1) logEventIndex
-- (2) logIndex
-- (3) logTime
-- (4) logDescription

4.3.5 Bridge-MIB (1.3.6.1.2.1.17)

4.3.5.1 dot1dBase (1.3.6.1.2.1.17.1)

Die dot1dBase-Gruppe enthält brückenspezifische Informationen.

(1) dot1dBaseBridgeAddress
(2) dot1dBaseNumPorts
(3) dot1dBasePortType
(4) dot1dBasePortTable
-- dot1dBasePortEntry
-- (1) dot1dBasePort
-- (2) dot1dBasePortIfIndex
-- (3) dot1dBasePortPortCircuit
-- (4) dot1dBasePortDelayExceededDiscards
-- (5) dot1dBasePortMtuExceededDiscards

4.3.5.2 dot1dStp (1.3.6.1.2.1.17.2)

-- (1) dot1dStpProtocolSpecification
-- (2) dot1dStpPriority
-- (3) dot1dStpTimeSinceTopologyChange
-- (4) dot1dStpTopChanges
-- (5) dot1dStpDesignateRoot
-- (6) dot1dStpRootCost
-- (7) dot1dStpRootPort
-- (8) dot1dStpMaxAge
-- (9) dot1dStpHelloTime
-- (10) dot1dStpHoldTime
-- (11) dot1dStpForwardDelay
-- (12) dot1dStpBridgeMaxAge
-- (13) dot1dStpBridgeHelloTime
-- (14) dot1dStpBridgeForwardDelay
-- (15) dot1dStpPortTable
-- (1) dot1dStpPortEntry
-- (1) dot1dStpPort
-- (2) dot1dStpPortPriority
-- (3) dot1dStpPortState
-- (4) dot1dStpPortEnable
-- (5) dot1dStpPortPathCost
-- (6) dot1dStpPortDesignatedRoot
-- (7) dot1dStpPortDesignatedCost
-- (8) dot1dStpPortDesignatedBridge
-- (9) dot1dStpPortDesignatedPort
-- (10) dot1dStpPortForwardTransitions
-- (11) dot1dStpPortPathCost32
-- (16) dot1dStpVersion
-- (17) dot1dStpTxHoldCount
-- (18) dot1dStpPathCostDefault
-- (19) dot1dStpExtPortTable

-- (1) dot1dStpExtPortEntry
-- (1) dot1dStpPortProtocolMigration
-- (2) dot1dStpPortAdminEdgePort
-- (3) dot1dStpPortOperEdgePort
-- (4) dot1dStpPortAdminPointToPoint
-- (5) dot1dStpPortOperPointToPoint
-- (6) dot1dStpPortAdminPathCost

4.3.5.3 dot1dTp (1.3.6.1.2.1.17.4)

Die dot1dTp-Gruppe enthält brückenspezifische Informationen.

(1) dot1dTpLearnedEntryDiscards
(2) dot1dTpAgingTime
(3) dot1dTpFdbTable
-- (1) dot1dTpFdbEntry
-- (1) dot1dTpFdbAddress
-- (2) dot1dTpFdbPort
-- (3) dot1dTpFdbStatus
(4) dot1dTpPortTable
-- dot1dTpPortEntry
-- (1) dot1dTpPort
-- (2) dot1dTpPortMaxInfo
-- (3) dot1dTpPortInFrames
-- (4) dot1dTpPortOutFrames
-- (5) dot1dTpPortInDiscards
(5) dot1dTpHCPortTable
-- dot1dTpHCPortEntry
-- (1) dot1dTpHCPortInFrames
-- (2) dot1dTpHCPortOutFrames
-- (3) dot1dTpHCPortInDiscards
(6) dot1dTpPortOverflowTable
-- dot1dTpPortOverflowEntry
-- (1) dot1dTpPortInOverflowFrames
-- (2) dot1dTpPortOutOverflowFrames
-- (3) dot1dTpPortInOverflowDiscards

4.3.5.4 dot1dStatic (1.3.6.1.2.1.17.5)

-- (1) dot1dStaticTable
-- (1) dot1dStaticEntry
-- (1) dot1dStaticAddress
-- (2) dot1dStaticReceivePort
-- (3) dot1dStaticAllowedToGoTo

4.3.6 pBridgeMIB (1.3.6.1.2.1.17.6)

4.3.6.1 pBridgeMIBObjects (1.3.6.1.2.1.17.6.1)

-- (1) dot1dExtBase
- -- (1) dot1dDeviceCapabilities
- -- (2) dot1dTrafficClassesEnabled
- -- (3) dot1dGmrpStatus
- -- (4) dot1dCapabilitiesTable
  - -- (1) dot1dCapabilitiesEntry
    - -- (1) dot1dPortCapabilities

-- (2) dot1dPriority
- -- (1) dot1dPortPriorityTable
  - -- (1) dot1dPortPriorityEntry
    - -- (1) dot1dPortDefaultUserPriority
    - -- (2) dot1dPortNumTrafficClasses
- -- (2) dot1dUserPriorityRegenTable
  - -- (1) dot1dUserPriorityRegenTable
    - -- (1) dot1dUserPriority
    - -- (2) dot1dRegenUserPriority
- -- (3) dot1dTrafficClassTable
  - -- (1) dot1dTrafficClassEntry
    - -- (1) dot1dTrafficClassPriority
    - -- (2) dot1dTrafficClass
- -- (4) dot1dPortOutboundAccessPriorityTable
  - -- (1) dot1dPortOutboundAccessPriorityEntry
    - -- (1) dot1dPortOutboundAccessPriority

-- (3) dot1dGarp
- -- (1) dot1dPortGarpTable
  - -- (1) dot1dPortGarpEntry
    - -- (1) dot1dPortGarpJoinTime
    - -- (2) dot1dPortGarpLeaveTime
    - -- (3) dot1dPortGarpLeaveAllTime

-- (4) dot1dGmrp
- -- (1) dot1dPortGmrpTable
  - -- (1) dot1dPortGmrpEntry
    - -- (1) dot1dPortGmrpStatus
    - -- (2) dot1dPortGmrpFailedRegistrations
    - -- (3) dot1dPortGmrpLastPduOrigin

4.3.6.2 pBridgeConformance (1.3.6.1.2.1.17.6.2)

-- (1) pBridgeGroups
- -- (1) pBridgeExtCapGroup
- -- (2) pBridgeDeviceGmrpGroup
- -- (3) pBridgeDevicePriorityGroup
- -- (4) pBridgeDefaultPriorityGroup
- -- (5) pBridgeRegentPriorityGroup
- -- (6) pBridgePriorityGroup
- -- (7) pBridgeAccessPriorityGroup

-- (8) pBridgePortGarpGroup
-- (9) pBridgePortGmrpGroup
-- (10) pBridgeHCPortGroup
-- (11) pBridgePortOverflowGroup
-- (2) pBridgeCompliances
-- (1) pBridgeCompliance

4.3.7 qBridgeMIB (1.3.6.1.2.1.17.7)

4.3.7.1 qBridgeMIBObjects (1.3.6.1.2.1.17.7.1)

-- (1) dot1qBase
-- (1) dot1qVLANVersionNumber
-- (2) dot1qMaxVLANId
-- (3) dot1qMaxSupportedVLANs
-- (4) dot1qNumVLANs
-- (5) dot1qGvrpStatus
-- (2) dot1qTp
-- (1) dot1qFdbTable
-- (1) dot1qFdbEntry
-- (1) dot1qFdbId
-- (2) dot1qFdbDynamicCount
-- (2) dot1qTpFdbTable
-- (1) dot1qTpFdbEntry
-- (1) dot1qTpFdbAddress
-- (2) dot1qTpFdbPort
-- (3) dot1qTpFdbStatus
-- (3) dot1qTpGroupTable
-- (1) dot1qTpGroupEntry
-- (1) dot1qTpGroupAddress
-- (2) dot1qTpGroupEgressPorts
-- (3) dot1qTpGroupLearnt
-- (4) dot1qForwardAllTable
-- (1) dot1qForwardAllEntry
-- (1) dot1qForwardAllPorts
-- (2) dot1qForwardAllStaticPorts
-- (3) dot1qForwardAllForbiddenPorts
-- (5) dot1qForwardUnregisteredTable
-- (1) dot1qForwardUnregisteredEntry
-- (1) dot1qForwardUnregisteredPorts
-- (2) dot1qForwardUnregisteredStaticPorts
-- (3) dot1qForwardUnregisteredForbiddenPorts
-- (3) dot1qStatic
-- (1) dot1qStaticUnicastTable
-- (1) dot1qStaticUnicastEntry
-- (1) dot1qStaticUnicastAddress
-- (2) dot1qStaticUnicastReceivePort
-- (3) dot1qStaticUnicastAllowedToGoTo
-- (4) dot1qStaticUnicastStatus

```
        -- (2) dot1qStaticMulticastTable
                -- (1) dot1qStaticMulticastEntry
                    -- (1) dot1qStaticMulticastAddress
                    -- (2) dot1qStaticMulticastReceivePort
                    -- (3) dot1qStaticMulticastStaticEgressPorts
                    -- (4) dot1qStaticMulticastForbiddenEgressPorts
                    -- (5) dot1qStaticMulticastStatus
    -- (4) dot1qVLAN
        -- (1) dot1qVLANNumDeletes
        -- (2) dot1qVLANCurrentTable
                -- (1) dot1qVLANCurrentEntry
                    -- (1) dot1qVLANTimeMark
                    -- (2) dot1qVLANIndex
                    -- (3) dot1qVLANFdbId
                    -- (4) dot1qVLANCurrentEgressPorts
                    -- (5) dot1qVLANCurrentUntaggedPorts
                    -- (6) dot1qVLANStatus
                    -- (7) dot1qVLANCreationTime
        -- (3) dot1qVLANStaticTable
                -- (1) dot1qVLANStaticEntry
                    -- (1) dot1qVLANStaticName
                    -- (2) dot1qVLANStaticEgressPorts
                    -- (3) dot1qVLANForbiddenEgressPorts
                    -- (4) dot1qVLANStaticUntaggedPorts
                    -- (5) dot1qVLANStaticRowStatus
        -- (4) dot1qNextFreeLocalVLANIndex
        -- (5) dot1qPortVLANTable
                -- (1) dot1qPortVLANEntry
                    -- (1) dot1qPvid
                    -- (2) dot1qPortAcceptableFrameTypes
                    -- (3) dot1qPortIngressFiltering
                    -- (4) dot1qPortGvrpStatus
                    -- (5) dot1qPortGvrpFailedRegistrations
                    -- (6) dot1qPortGvrpLastPduOrigin
        -- (6) dot1qPortVLANStatisticsTable
                -- (1) dot1qPortVLANStatisticsEntry
                    -- (1) dot1qTpVLANPortInFrames
                    -- (2) dot1qTpVLANPortOutFrames
                    -- (3) dot1qTpVLANPortInDiscards
                    -- (4) dot1qTpVLANPortInOverflowFrames
                    -- (5) dot1qTpVLANPortOutOverflowFrames
                    -- (6) dot1qTpVLANPortInOverflowDiscards
        -- (7) dot1qPortVLANHCStatisticsTable
                -- (1) dot1qPortVLANHCStatisticsEntry
                    -- (1) dot1qPortVLANHCInFrames
                    -- (2) dot1qPortVLANHCOutFrames
                    -- (3) dot1qPortVLANHCIn Discards
        -- (8) dot1qLearningConstraintsTable
                -- (1) dot1qLearningConstraintsEntry
                    -- (1) dot1qConstraintVLAN
```

-- (2) dot1qConstraintSet
-- (3) dot1qConstraintType
-- (4) dot1qConstraintStatus
-- (9) dot1qConstraintSetDefault
-- (10) dot1qConstraintTypeDefault

4.3.7.2 qBridgeConformance (1.3.6.1.2.1.17.7.2)

-- (1) qBridgeGroups
-- (1) qBridgeBaseGroup
-- (2) qBridgeFdbUnicastGroup
-- (3) qBridgeFdbMulticastGroup
-- (4) qBridgeServiceRequirementsGroup
-- (5) qBridgeFdbStaticGroup
-- (6) qBridgeVLANGroup
-- (7) qBridgeVLANStaticGroup
-- (8) qBridgePortGroup
-- (9) qBridgeVLANStatisticsGroup
-- (10) qBridgeVLANStatisticsOverflowGroup
-- (11) qBridgeVLANHCStatisticsGroup
-- (12) qBridgeLearningConstraintsGroup
-- (13) qBridgeLearningConstraintDefaultGroup
-- (2) qBridgeCompliances
-- (1) qBridgeCompliance

4.3.7.3 dot1dConformance (1.3.6.1.2.1.17.7.3)

-- (1) dot1dGroups
-- (1) dot1dBaseBridgeGroup
-- (2) dot1BasePortGroup
-- (3) dot1dStpBridgeGroup
-- (4) dot1dStpPortGroup2
-- (5) dot1dStpPortGroup3
-- (6) dot1dTpBridgeGroup
-- (7) dot1dTpSdbGroup
-- (8) dot1dTpGroup
-- (9) dot1dStaticGroup
-- (10) dot1dNotificationGroup
-- (2) dot1dCompliances
-- (1) BridgeCompliances1493
-- (2) BridgeCompliances4188

4.3.8 rstp MIB (1.3.6.1.2.1.17.11)

4.3.8.1 rstp Conformance (1.3.6.1.2.1.17.11.1)

rstp Groups (1.3.6.1.2.1.17.11.1.1)

-- (1) rstpBridgeGroups
-- (2) rstpDefaultPathCostGroup
-- (3) rstpPortGroup

rstp Compliances Groups (1.3.6.1.2.1.17.11.1.2)

-- (1) rstpCompliance

4.3.9 IANAifType-MIB (1.3.6.1.2.1.30)

Die IANAifType-MIB definiert die „ifTable“ in der MIB II. Siehe „Interface-Gruppe (1.3.6.1.2.1.2)“ auf Seite 4-48.

4.3.10 IF-MIB (1.3.6.1.2.1.31)

4.3.10.1 ifMIBObjects (1.3.6.1.2.1.31.1)

-- (1) ifXTable
  -- (1) ifXEntry
    -- (1) ifName
    -- (2) ifInMulticastPkts
    -- (3) ifInBroadcastPkts
    -- (4) ifOutMulticastPkts
    -- (5) ifOutBroadcastPkts
    -- (6) ifHCInOctets
    -- (7) ifHCInUcastPkts
    -- (8) ifHCInMulticastPkts
    -- (9) ifHCInBroadcastPkts
    -- (10) ifHCOutOctets
    -- (11) ifHCOutUcastPkts
    -- (12) ifHCOutMulticastPkts
    -- (13) ifHCOutBroadcastPkts
    -- (14) ifLinkUpDownTrapEnable
    -- (15) ifHighSpeed
    -- (16) ifPromiscuousMode
    -- (17) ifConnectorPresent
    -- (18) ifAlias
    -- (19) ifCounterDiscontinuityTime
-- (2) ifStackTable
  -- (1) ifStackEntry
    -- (1) ifStackHigherLayer
    -- (2) ifStackLowerLayer
    -- (3) ifStackStatus
-- (3) ifTestTable
  -- (1) ifTestEntry
    -- (1) ifTestID
    -- (2) ifTestStatus
    -- (3) ifTestType
    -- (4) ifTestResult
    -- (5) ifTestCode
    -- (6) ifTestOwner
-- (4) ifRcvAddressTable
  -- (1) ifRcvAddressEntry

-- (1) ifRcvAddressAddress
-- (2) ifRcvAddressStatus
-- (3) ifRcvAddressType
-- (5) ifTableLastChange
-- (6) ifStackLastChange

4.3.10.2 ifConformance (1.3.6.1.2.1.31.2)

-- (1) ifGroups
-- (1) ifGeneralGroup
-- (2) ifFixedLengthGroup
-- (3) ifHCFixedLengthGroup
-- (4) ifPacketGroup
-- (5) ifHCPacketGroup
-- (6) ifVHCPacketGroup
-- (7) ifRcvAddressGroup
-- (8) ifTestGroup
-- (9) ifStackGroup
-- (10) ifGeneralInformationGroup
-- (11) ifStackGroup2
-- (12) ifOldObjectsGroup
-- (13) ifCounterDiscontinuityGroup
-- (2) ifCompliances
-- (1) ifCompliance
-- (2) ifCompliance2

4.3.10.3 etherMIBObjects (1.3.6.1.2.1.32.1)

-- (1) etherConformance
-- (1) etherGroups
-- (1) etherStatsGroup
-- (2) etherCollisionTableGroup
-- (3) etherStats100BbsGroup
-- (4) etherStatsBaseGroup
-- (5) etherStatsLowSpeedGroup
-- (6) etherStatsHighSpeedGroup
-- (7) etherDuplexGroup
-- (8) etherControlGroup
-- (9) etherControlPauseGroup
-- (1) etherCompliances
-- (1) etherCompliances
-- (2) ether100MbsCompliance
-- (3) dot3Compliance

4.3.10.4 lldpMIB (1.0.8802.1.1.2)

(1) lldpObjects
-- (1) lldpConfiguration
    -- (1) lldpMessageTxInterval
    -- (2) lldpMessageTxHoldMultiplier
-- (2) lldpStatistics
-- (3) lldpLocalSystemData
    -- (1) lldpLocChassisIdSubType
    -- (2) lldpLocChassisId
    -- (3) lldpLocSysName
    -- (4) lldpLocSysDesc
    -- (5) lldpLocSysCapSupported
    -- (6) lldpLocSysCapEnabled
    -- (7) lldpLocPortTable
        -- (1) lldpLocPortMum
        -- (2) lldpLocPortIdSubtype
        -- (3) lldpLocPortId
        -- (4) lldpLocPortDesc
    -- (8) lldpLocManAddrTable
        -- (1) lldpLocManAddrSubtype
        -- (2) lldpLocManAddr
        -- (3) lldpLocManAddrLen
        -- (4) lldpLocManAddrIfSubtype
        -- (5) lldpLocManAddrIfId
        -- (6) lldpLocManAddrOID
-- (4) lldpRemoteSystemsData
    -- (1) lldpRemTable
        -- (1) lldpRemTimeMark
        -- (2) lldpRemLocalPortNum
        -- (3) lldpRemIndex
        -- (4) lldpRemChassisType
        -- (5) lldpRemChassisId
        -- (6) lldpRemPortIdSubtype
        -- (7) lldpRemPortId
        -- (8) lldpRemPortDesc
        -- (9) lldpRemSysName
        -- (10) lldpRemSysDesc
        -- (11) lldpRemSysCapSupported
        -- (12) lldpRemSysCapEnabled
    -- (2) lldpRemManAddrTable
        -- (1) lldpRemAddrSubSubtype
        -- (2) lldpRemManAddr
        -- (3) lldpRemManAddrIfSubtype
        -- (4) lldpRemManAddrIfId
        -- (5) lldpRemManAddrOID
-- (5) lldpConformance

4.3.11 pnoRedundancy.mib

(1) pnoMRPDomainTable
-- (1) pnoMRPDomainEntry
-- (1) pnoMRPDomainIndex
-- (2) pnoMRPDomainUuid
-- (3) pnoMRPDomainName
-- (4) pnoMRPDomainAdminRole
-- (5) pnoMRPDomainOperRole
-- (6) pnoMRPDomainManagerPriority
-- (7) pnoMRPDomainRingPort1
-- (8) pnoMRPDomainRingPort1State
-- (9) pnoMRPDomainRingPort2
-- (10)pnoMRPDomainRingPort2State
-- (11) pnoMRPDomainState
-- (12) pnoMRPDomainError
-- (13) pnoMRPDomainRingOpenCount
-- (14) pnoMRPDomainLastRingOpenChange
-- (15) pnoMRPDomainRoundTripDelayMax
-- (16) pnoMRPDomainRoundTripDelayMin
-- (17) pnoMRPDomainResetRoundTripDelays

4.3.12 Private MIBs

Die privaten MIBs für den MMS von Phoenix Contact finden Sie unter der Object-ID 1.3.6.1.4.1.4346. Die MIB des MMS enthält die Gruppen:

– pxcModules (OID = 1.3.6.1.4.1.4346.1),
– pxcGlobal (OID = 1.3.6.1.4.1.4346.2) und
– pxcFactoryLine (OID = 1.3.6.1.4.1.4346.11)

Alle Konfigurationsänderungen, die nach einem Neustarts des MMS wirksam sein sollen, müssen mit Hilfe des Objekts „flWorkFWCtrlConfSave“ dauerhaft gespeichert werden.

Die Aging Time (Default: 40 Sekunden) wird nicht über die Private MIBs verstellt, sondern über das MIB-Objekt „dot1dTpAgingTime“ (OID 1.3.6.1.2.1.17.4.2). Der mögliche Einstellbereich ist 10 - 825 Sekunden.

MIB-Tree

So ist die private MIB von Phoenix Contact in den MIB-Tree integriert (siehe roten Pfeil).

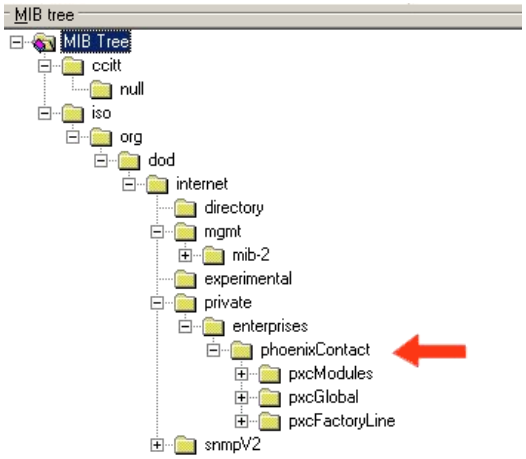


Bild 4-49 MIB-Tree

4.3.12.1 pxcModules OID = 1.3.6.1.4.1.4346.1

flMSwitchMModule

OID 1.3.6.1.4.1.4346.1.8

Das Objekt enthält Informationen zum Hersteller.

4.3.12.2 pxcGlobal OID = 1.3.6.1.4.1.4346.2

pxcBasic

OID 1.3.6.1.4.1.4346.2.1

	pxcBasicName
OID	1.3.6.1.4.1.4346.2.1.1
Syntax	Display String
Zugriff	lesen
Beschreibung	Liefert den Namen des Herstellers: Phoenix Contact GmbH & Co. KG.
	pxcBasicDescr
OID	1.3.6.1.4.1.4346.2.1.2
Syntax	Display String
Zugriff	lesen
Beschreibung	Liefert den Namen und die Anschrift des Herstellers: Phoenix Contact GmbH & Co. KG P.O. Box 1341 D-32819 Blomberg.
	pxcBasicURL
OID	1.3.6.1.4.1.4346.2.1.3
Syntax	Display String
Zugriff	lesen
Beschreibung	Liefert die Internet-Adresse des Herstellers: http://www.phoenixcontact.com.

4.3.12.3 pxcFactoryLine OID = 1.3.6.1.4.1.4346.11

	flGlobal
OID	1.3.6.1.4.1.4346.11.1
	flBasic
OID	1.3.6.1.4.1.4346.11.1.1
	flBasicName
OID	1.3.6.1.4.1.4346.11.1.1.1
Syntax	Display String
Zugriff	lesen
Beschreibung	Liefert die Bezeichnung der Produktgruppe: Factory Line.

	flBasicDescr
OID	1.3.6.1.4.1.4346.11.1.1.2
Syntax	Display String
Zugriff	lesen
Beschreibung	Liefert eine Kurzbeschreibung der Produktgruppe: Ethernet Installation System.
	flBasicURL
OID	1.3.6.1.4.1.4346.11.1.1.3
Syntax	Display String
Zugriff	lesen
Beschreibung	Liefert eine spezifische URL der Produktgruppe: www.factoryline.de.
	flBasicCompCapacity
OID	1.3.6.1.4.1.4346.11.1.1.4
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Enthält die Anzahl der unterschiedlichen Komponenten, die mit diesem Gerät verwaltet werden können.
	flComponents
OID	1.3.6.1.4.1.4346.11.1.2
	flComponentsTable
OID	1.3.6.1.4.1.4346.11.1.2.1
	flComponentsTableEntry

OID	1.3.6.1.4.1.4346.11.1.2.1.1
Syntax	
Zugriff	
Beschreibung	Generiert eine Tabelle mit den Komponenten-Beschreibungen der Produktgruppe „Factory Line“, die von dieser Management-Einheit verwaltet werden können.
flComponentsIndex	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen

Beschreibung	Nennt den Produktindex der Komponente.
flComponentsName	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.2
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Zeigt die Bezeichnung der Komponente.
flComponentsDescr	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.3
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert eine Kurzbeschreibung der Komponente.
flComponentsURL	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.4
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert die URL einer Webseite mit weiterführenden Informationen www.factoryline.de.
flComponentsOrderNumber	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.5
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert die Artikel-Nummer der Komponente.

flWorkDevice

OID 1.3.6.1.4.1.4346.11.11

flWorkBasic

OID 1.3.6.1.4.1.4346.11.11.1

flWorkBasicName

OID	1.3.6.1.4.1.4346.11.11.1.1
Syntax	DisplayString
Zugriff	lesen und schreiben
Beschreibung	Liefert den Gerätenamen (entspricht „sysName“ aus MIB2).

flWorkBasicDescr

OID	1.3.6.1.4.1.4346.11.11.1.2
Syntax	DisplayString
Zugriff	lesen und schreiben
Beschreibung	Liefert eine Kurzbeschreibung (entspricht „sysDescr“ aus MIB2).

flWorkBasicURL

OID	1.3.6.1.4.1.4346.11.11.1.3
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert die URL der geräteeigenen Webseite des WBM in Form der zurzeit eingestellten IP-Adresse.

flWorkBasicSerialNumber

OID	1.3.6.1.4.1.4346.11.11.1.4
Syntax	Octet String (12)
Zugriff	lesen
Beschreibung	Liefert die Seriennummer des Gerätes.

flWorkBasicHWRevision

OID	1.3.6.1.4.1.4346.11.11.1.5
Syntax	Octet String (4)
Zugriff	lesen
Beschreibung	Liefert die Hardware-Version des Gerätes.

flWorkBasicPowerStat

OID	1.3.6.1.4.1.4346.11.11.1.6
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Liefert eine Status-Information über die angeschlossen Versorgungsspannungen: Unbekannt 1 Versorgungsspannung 1 OK 3 Versorgungsspannung 2 OK 4 Versorgungsspannung 1 und 2 OK 5

flWorkBasicSystemBusRevision

OID	1.3.6.1.4.1.4346.11.11.1.7
Syntax	Octet String (4)
Zugriff	lesen
Beschreibung	Liefert die Revisions-Kennung des Systembusses.

flWorkBasicCompMaxCapacity

OID	1.3.6.1.4.1.4346.11.11.1.11
Syntax	Integer 32
Zugriff	lesen
Beschreibung	Liefert die maximale Anzahl der anschließbaren Interfaces.

flWorkBasicCompCapacity

OID	1.3.6.1.4.1.4346.11.11.1.12
Syntax	Integer 32
Zugriff	lesen
Beschreibung	Liefert die Anzahl der tatsächlich angeschlossenen Interfaces.

flWorkComponents

OID	1.3.6.1.4.1.4346.11.11.2

flWorkComponentsTable

OID	1.3.6.1.4.1.4346.11.11.2.1

flWorkComponentsEntry

OID	1.3.6.1.4.1.4346.11.11.2.1.1
Beschreibung	Generiert eine Tabelle mit den verfügbaren Interfaces-Modulen dieser Switch-Station
flWorkComponentsIndex	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Nennt die gewählte Interface-Nummer.
flWorkComponentsOID	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.2
Syntax	OBJECT IDENTIFIER
Zugriff	lesen
Beschreibung	Diese OID zeigt den zugehörigen Eintrag in flWorkComponentsEntry
flWorkComponentsURL	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.3
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert die IP-Adresse des Switches.
flWorkComponentsDevSign	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.4
Syntax	Integer (0 ... 24)
Zugriff	lesen
Beschreibung	Liefert die Bezeichnung des Interface-Modules.

flWorkTraps

OID 1.3.6.1.4.1.4346.11.11.3

flWorkTrapsDelemeter

OID 1.3.6.1.4.1.4346.11.11.3.0

trapPasswdAccess

OID 1.3.6.1.4.1.4346.11.11.3.0.1

Beschreibung Wird bei jeder Änderung oder jedem Änderungsversuch auf das Geräte-Passwort an die definierten Trap-Receiver gesendet und enthält eine Information zum Status der letzten Änderung oder des letzten Änderungsversuchs.

trapFWHealth

OID 1.3.6.1.4.1.4346.11.11.3.0.2

Beschreibung Wird bei jeder Firmware-relevanten Änderung des Diagnose-Displays gesendet und enthält weitere Informationen zum Firmware-Status.

trapFWConf

OID 1.3.6.1.4.1.4346.11.11.3.0.3

Beschreibung Wird bei jedem Speichern der Konfiguration gesendet und informiert so die Management-Station über die erfolgreiche Konfigurationsspeicherung.
Dieser Trap wird bei Konfigurationsänderungen (Port-Name, Port-Modus, Gerätename, IP-Adresse, Trap-Receiver-Adresse, Port-Mirroring o.ä.), die noch nicht dauerhaft gespeichert sind, verschickt. Der Trap stellt somit eine Warnung dar, dass die Änderungen (ohne eine dauerhafte Speicherung) nach einem Reset verloren sind.

Das Objekt „flWorkNetIfParamAssignment“ muss auf statisch (1) stehen, sonst ist das Beschreiben der Objekte nicht möglich.

trapPowerSupply

OID 1.3.6.1.4.1.4346.11.11.3.0.4

Beschreibung Wird bei jedem Ausfall der redundanten Spannungseinspeisung gesendet.

trapSecurityPort

OID 1.3.6.1.4.1.4346.11.11.3.0.5

Beschreibung Wird bei jedem Zugriff einer nicht freigegebenen MAC-Adresse auf einen Port versendet.

trapRstpRingFailure

OID 1.3.6.1.4.1.4346.11.11.3.0.6

Beschreibung Wird bei einer Link-Unterbrechung im redundanten RSTP-Ring versendet.

trapPofScrjPort

OID	1.3.6.1.4.1.4346.11.11.3.0.7
Beschreibung	Wird beim Wechsel in einen oder aus einem kritischen Zustand versendet.

trapPoEPort

OID	1.3.6.1.4.1.4346.11.11.3.0.8
Beschreibung	Wird immer dann versendet, wenn sich der Fehlerstatus eines PoE-Ports verändert.

trapManagerConnection

OID	1.3.6.1.4.1.4346.11.11.3.0.99
Beschreibung	Dieser Trap wird zum Testen der Verbindung zwischen Gerät und Trap-Manager benutzt.

flWorkNet

OID	1.3.6.1.4.1.4346.11.11.4

flWorkNetIfParameter

OID	1.3.6.1.4.1.4346.11.11.4.1

flWorkNetIfParamPhyAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.1
Syntax	MacAddress
Zugriff	lesen
Beschreibung	Liefert die MAC-Adresse des Switches.

flWorkNetIfParamIPAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.2
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Liefert die zurzeit eingestellte IP-Adresse des MMS. Änderungen werden erst nach Ausführung des Objects „flWorkNetIfParamSave“ wirksam.

Das Objekt „flWorkNetIfParamAssignment“ muss auf statisch (1) stehen, sonst ist das Beschreiben der Objekte nicht möglich.

flWorkNetIfParamSubnetmask

OID	1.3.6.1.4.1.4346.11.11.4.1.3

Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Liefert die zurzeit eingestellte Subnetz-Maske des MMS. Änderungen werden erst nach Ausführung des Objects „flWorkNetIfParamSave“ wirksam.

Das Objekt „flWorkNetIfParamAssignment“ muss auf statisch (1) stehen, sonst ist das Beschreiben der Objekte nicht möglich.

flWorkNetIfParamGwIpAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.4
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Liefert die IP-Adresse des zurzeit eingestellten Default-Gateway/Router des MMS. Änderungen werden erst nach Ausführung des Objects „flWorkNetIfParamSave“ wirksam.

Das Objekt „flWorkNetIfParamAssignment“ muss auf statisch (1) stehen, sonst ist das Beschreiben der Objekte nicht möglich.

flWorkNetIfParamStatus

OID	1.3.6.1.4.1.4346.11.11.4.1.5
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Zeigt, ob IP-Parameter verändert, aber nicht gespeichert wurden:

Keine Veränderung	1
Adresseinstellung geändert, aber noch nicht aktiviert	2

Adresseinstellungen müssen dauerhaft über das Objekt „flWorkFWCtrlConfSave“ gespeichert werden.

flWorkNetIfParamSave

OID	1.3.6.1.4.1.4346.11.11.4.1.6
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Ermöglicht, die geänderten IP-Parameter zu speichern oder die Änderung zurückzunehmen:

Änderung rückgängig machen	1
Änderung aktivieren	2

Adresseinstellungen müssen dauerhaft über das Objekt „flWorkFWCtrlConfSave“ gespeichert werden.

flWorkNetIfParamAssignment

OID	1.3.6.1.4.1.4346.11.11.4.1.7
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Ermöglicht, den Vergabemechanismus der IP-Parameter zu verändern.

Statische IP-Adresse 1
Vergabe per BootP 2
Vergabe per DHCP 3
Vergabe per DCP 4

Änderungen des Vergabemechanismus haben auch Auswirkungen auf die Management-Funktionen über das Web-Interface, über V.24 und Telnet.

Die Änderungen des Vergabemechanismus auf BootP (2) oder auf DCP (4) werden erst nach einem Neustart des MMS aktiv.

Adresseinstellungen müssen dauerhaft über das Objekt „flWorkFWCtrlConfSave“ gespeichert werden.

flWorkNetIfParamManagementVlanId

OID	1.3.6.1.4.1.4346.11.11.4.1.8
Syntax	Integer32 (1 ... 4094)
Zugriff	lesen und schreiben
Beschreibung	Wenn der Switch im VLAN-Modus „Tagging“ betrieben wird, zeigt dieses Objekt, im welchen VLAN (VLAN-ID) sich der Management-Agent befindet.

flWorkNetPort

OID 1.3.6.1.4.1.4346.11.11.4.2

flWorkNetPortCapacity

OID	1.3.6.1.4.1.4346.11.11.4.2.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Liefert die Anzahl der verfügbaren Ports in Abhängigkeit der Konfiguration des MMS.

flWorkNetPortTable

OID 1.3.6.1.4.1.4346.11.11.4.2.2

flWorkNetPortEntry

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1
Beschreibung	Generiert eine Tabelle mit einer detaillierten Beschreibung der Port-Konfiguration.
flWorkNetPortIndex	

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Nennt die Port-Nummer des gewählten Ports.
flWorkNetPortLinkState	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.2
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Port-Status: Verbunden 1 Nicht verbunden 2 farEndFault 3
flWorkNetPortSpeed	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.3
Syntax	Gauge32
Zugriff	lesen
Beschreibung	Liefert die Datenübertragungsrate des gewählten Ports in Bit/s.
flWorkNetPortDuplexMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.4
Syntax	Integer
Zugriff	lesen
Beschreibung	Liefert den Duplex-Mode des gewählten Ports: Kein Link 0 Vollduplex 1 Halbduplex 2
flWorkNetPortNegotiation	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.5
Syntax	Integer
Zugriff	lesen
Beschreibung	Liefert den Duplex-Mode des gewählten Ports: Automatisch 1 Manuell 2
flWorkNetPortName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.6
Syntax	Octet String (0 ... 16)
Zugriff	lesen und schreiben
Beschreibung	Liefert den „Namen“ des Ports, z.B. „Roboter 1“.
flWorkNetPortEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.7
Syntax	Integer
Zugriff	lesen und schreiben

Beschreibung	Hier können Sie den Port abschalten: Port abgeschaltet 1 Port eingeschaltet 2
flWorkNetPortLinkMonitoring	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.8
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Mit diesem Object kann Link-Monitoring (Meldung über Display und Meldekontakt) für den entsprechenden Port eingeschaltet werden: Link-Monitoring eingeschaltet 2 Link-Monitoring ausgeschaltet 1
flWorkNetPortModus	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.9
Syntax	Integer32 (0 ... 1024)
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Übertragungsmodus des entsprechenden Ports eingestellt werden: Autonegotiation1 10 MBit/s halbduplex 2 10 MBit/s vollduplex 3 100 MBit/s halbduplex 4 100 MBit/s vollduplex 5
	Bei Glasfaser-FX-Ports ist nur 100 MBit/s vollduplex (5) möglich.
	Die Autocrossing-Funktion ist nur bei eingeschalteten Auto-Negotiation aktiv. Wenn Sie die Übertragungsgeschwindigkeit oder den Übertragungsmodus fest einstellen, wird die Autocrossing-Funktion abgeschaltet.
flWorkNetPortSTPEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.10
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Dieses Objekt regelt den Umgang mit BPDUs, wenn (Rapid) Spanning Tree aktiviert ist: **Firmware mit Rapid Spanning Tree Protocol:** RSTP nicht aktiviert 1 RSTP aktiviert 2 **Firmware mit Spanning Tree Protocol:** STP nicht aktiviert (Port befindet sich im Fast-Forwarding-Modus 1 STP aktiviert 2
flWorkNetPortIfIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.11
Syntax	Integer32 (0 ... 1024)
Zugriff	lesen

Beschreibung	Nennt den Index des Ports gemäß IEEE 802.3ad.
flWorkNetLLWHPort	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.12
Syntax	Integer32 (8193 ... 8296)
Zugriff	lesen
Beschreibung	Nennt den Index des Ports gemäß IEEE 802.3ad, jedoch evtl. mit Lücken (wegen fehlender Ports).
flWorkNetPortType	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.13
Syntax	Octet String
Zugriff	lesen
Beschreibung	Nennt das Medium dieses Ports.
flWorkNetPortModuleName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.14
Syntax	Octet String
Zugriff	lesen
Beschreibung	Nennt den „Namen“ des Moduls.
flWorkNetPortInterfaceName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.15
Syntax	Octet String
Zugriff	lesen
Beschreibung	Nennt den „Namen“ des Interfaces.
flWorkNetPortPriorityLevel	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.16
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Wählt die Prioritätsstufe für ankommende Datenpakete: Priorität niedrig 1 (Default) Priorität hoch 2
flWorkNetPortPofTransmittingPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.17
Syntax	Integer
Zugriff	lesen
Beschreibung	Für POF-LWL-Strecken <20 m muss die Sendeleistung abgesenkt werden. Mit diesem Objekt kann die Schalterstellung auf dem Interface-Modul ausgelesen werden. Sendeleistung unbekannt 1 Sendeleistung abgesenkt (Schalterstellung „OFF“) 2 Sendeleistung normal (Schalterstellung „ON“ 3
flWorkNetPortStpMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.18

Syntax	Integer
Zugriff	lesen
Beschreibung	Nennt den Modus des Ports bei Redundanz-Betrieb: Spanning Tree 1 Rapid Spanning Tree 2

flWorkNetPortPoETable

OID 1.3.6.1.4.1.4346.11.11.4.2.3

flWorkNetPortPoEEntry

OID	1.3.6.1.4.1.4346.11.11.4.2.3.1
Beschreibung	Generiert eine Tabelle mit einer detaillierten Beschreibung der PoE-Port-Konfiguration.
flWorkNetPortPoEIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Nennt die Port-Nummer des gewählten Ports.
flWorkNetPortPoEPowerEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt den Status des Ports in Bezug auf die PoE-Funktionalität: Der Port kann bei Bedarf Energie liefern 1 Der Port wird auch bei Bedarf **keine** Energie liefern 2 Der PoE-Status ist unbekannt und kann auch nicht eingestellt werden 3
flWorkNetPortPoECurrentLimitation	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Mit diesem Objekt kann die PoE-Strombegrenzung eingestellt werden: Begrenzung auf Class-1-Geräte oder 90 mA 1 Keine Begrenzung bis zum maximal zulässigen Wert (350 mA) 2 Der PoE-Status ist unbekannt und kann auch nicht eingestellt werden 3
flWorkNetPortPoEDeviceClass	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.4
Syntax	Integer (0 ... 5)
Zugriff	lesen

Beschreibung	Dieses Objekt liefert die detektierte PoE-Klasse des angeschlossenen Gerätes an den gewählten Port: Class 0 0 Class 1 1 Class 2 2 Class 3 3 Class 4 4 Class 5 5
flWorkNetPortPoEOutputCurrent	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.5
Syntax	Integer (1 ... 400)
Zugriff	lesen
Beschreibung	Dieses Objekt enthält den aktuellen Wert des Ausgangsstromes im „mA“ des gewählten Ports.
flWorkNetPortPoEOutputVoltage	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.6
Syntax	Integer32 (45000 ... 56000)
Zugriff	lesen
Beschreibung	Liefert die aktuelle Ausgangsspannung an diesem Port in „mV“.
flWorkNetPortPoEFaultStatus	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.7
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier erhalten Sie den aktuellen Fehlerstatus dieses Ports: Kein Fehler 0 Fehler in der externen PoE-Versorgungsspannung 1 Temperatur zu hoch 2 Strombegrenzung aktiviert 3 Load disconnected 4 Der PoE-Controller reagiert nicht, evtl. fehlt die 48-V-Versorgung 5 Kein PoE-Interface-Module an diesem Platz gesteckt 6 Der Switch unterstützt keine PoE-Interface-Module 7 Kein PoE-Verbraucher an diesem Port angeschlossen 8
flWorkNetPortPoEFaultMonitoring	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.8
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Mit diesem Object kann das PoE-Fault-Monitoring (Meldung über Display und Meldekontakt) für den entsprechenden Port eingeschaltet werden: Fault-Monitoring eingeschaltet 2 Fault-Monitoring ausgeschaltet 1

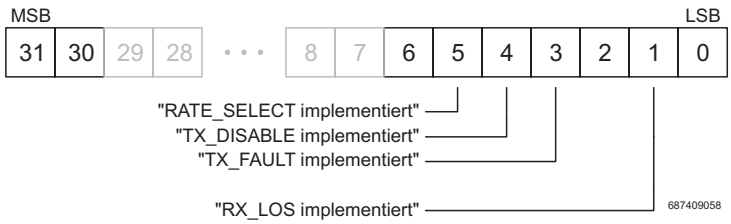
flWorkNetPofScrjIfGroup

OID	1.3.6.1.4.1.4346.11.11.4.2.4

flWorkNetPortPofScrjIfTable

OID	1.3.6.1.4.1.4346.11.11.4.2.4
Beschreibung	Generiert eine Tabelle mit einer detaillierten Beschreibung der POF-SCRJ-Port-Eigenschaften.
flWorkNetPortPofScrjIfIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Nennt die Port-Nummer des gewählten Ports.
flWorkNetPortPofScrjIfStatus	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.2
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Status des Ports in Bezug auf die POF-SCRJ-Funktionalität: Die Hardware unterstützt keine POF-SCRJ-Diagnose 1 An diesem Port befindet sich kein POF-SCRJ-Interface-Modul 2 Die Systemreserve an diesem Port ist größer 2 dB 3 Die Systemreserve ist kleiner 2 dB, aber größer 0 dB 4 Keine Systemreserve vorhanden - die empfangene Lichtleistung liegt unterhalb des erforderlichen Mindestwertes 5
flWorkNetPortPofScrjIfSupplyVoltage	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.4
Syntax	Integer32 (0 ... 65)
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die aktuelle Versorgungsspannung des Transceivers an diesem Port in 0,1 V -Schritten (möglicher Bereich: 0 V bis 6,5 V).
flWorkNetPortPofScrjIfTxPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.6
Syntax	Integer32 (0 ... 6553)
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die aktuelle Sendeleistung des Transceivers an diesem Port in 0,1 µW-Schritten (möglicher Bereich: 0 W bis 0,006553 W).
flWorkNetPortPofScrjIfRxPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.7
Syntax	Integer32 (0 ... 6553)
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die aktuelle Empfangsleistung des Transceivers an diesem Port in 0,1 µW-Schritten (möglicher Bereich: 0 W bis 0,006553 W).
flWorkNetPortPofScrjIfSystemReserve	

OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.8
Syntax	Integer32 (0 ... 255)
Zugriff	lesen
Beschreibung	Liefert die verbleibende Systemreserve in 0,1 dB-Schritten.
flWorkNetPortPofScrjIfRxPowerHighAlarm	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.9
Syntax	Integer
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt, ob der Alarm „RX power high“ ausgelöst ist: Alarm ist nicht ausgelöst 1 Alarm ist aus gelöst 2
flWorkNetPortPofScrjIfRxPowerLowAlarm	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.10
Syntax	Integer
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt, ob der Alarm „RX power low“ ausgelöst ist: Alarm ist nicht ausgelöst 1 Alarm ist aus gelöst 2
flWorkNetPortPofScrjIfRxPowerHighWarning	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.11
Syntax	Integer
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt, ob die Warnmeldung „RX power high“ ausgelöst ist: Warnmeldung ist nicht ausgelöst 1 Warnmeldung ist aus gelöst 2
flWorkNetPortPofScrjIfRxPowerLowWarning	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.12
Syntax	Integer
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt, ob die Warnmeldung „RX power low“ ausgelöst ist: Warnmeldung ist nicht ausgelöst 1 Warnmeldung ist aus gelöst 2
flWorkNetPortPofScrjIfManufacturer	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.13
Syntax	Octet String
Zugriff	lesen
Beschreibung	Dieses Objekt liefert den Namen des Herstellers des POF-SCRJ-Transceivers an diesem Port.
flWorkNetPortPofScrjIfManufactOui	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.14
Syntax	Octet String

Zugriff	lesen
Beschreibung	Dieses Objekt liefert die IEEE-Hersteller-Kennung des Herstellers des POF-SCRJ-Transceivers an diesem Port.
flWorkNetPortPofScrjIfRevision	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.16
Syntax	Octet String
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die Revision des POF-SCRJ-Transceivers an diesem Port.
flWorkNetPortPofScrjIfWavelength	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.17
Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die Wellenlänge in nm des POF-SCRJ-Transceivers an diesem Port.
flWorkNetPortPofScrjIfTransceiverOptions	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.18
Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die implementierten Funktionen des POF-SCRJ-Transceivers an diesem Port als Bit-Muster. 
flWorkNetPortPofScrjIfSerialNumber	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.19
Syntax	Octet String
Zugriff	lesen
Beschreibung	Dieses Objekt liefert die Seriennummer des POF-SCRJ-Transceivers an diesem Port.
flWorkNetPortPofScrjIfDatecodeAndLot	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.20
Syntax	Octet
Zugriff	lesen
Beschreibung	Dieses Objekt liefert das Herstellungsdatum und die Liefernummer des POF-SCRJ-Transceivers an diesem Port als Byte-Muster. Byte 1 und 2: Jahr Byte 3 und 4: Monat Byte 5 und 6: Tag Byte 7 und 8: Liefernummer

flWorkFirmware

OID	1.3.6.1.4.1.4346.11.11.11

flWorkFWInfo

OID	1.3.6.1.4.1.4346.11.11.11.1

flWorkFWInfoVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.1
Syntax	Octet String (4)
Zugriff	lesen
Beschreibung	Liefert die Firmware-Version als String. Beispiel für Version „3.97“: 0x33, 0x2e, 0x39, 0x37.

flWorkFWInfoState

OID	1.3.6.1.4.1.4346.11.11.11.1.2
Syntax	Octet String (6)
Zugriff	lesen
Beschreibung	Liefert das Firmware-Release als String. Beispiel für „beta“: 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoDate

OID	1.3.6.1.4.1.4346.11.11.11.1.3
Syntax	Octet String (6)
Zugriff	lesen
Beschreibung	Liefert das Erstellungsdatum der Firmware-Version als String. Beispiel für „21.05.2001“: 0x32, 0x31, 0x30, 0x35, 0x30, 0x31.

flWorkFWInfoTime

OID	1.3.6.1.4.1.4346.11.11.11.1.4
Syntax	Octet String (6)
Zugriff	lesen
Beschreibung	Liefert die Erstellungsuhrzeit der Firmware-Version als String. Beispiel für „14:10:20“: 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWInfoCopyright

OID	1.3.6.1.4.1.4346.11.11.11.1.5
Syntax	DisplayString (6)
Zugriff	lesen
Beschreibung	Liefert den Eigentümer des Firmware-Copyrights. Copyright by Phoenix Contact GmbH & Co., 2003.

flWorkFWInfoBootVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.6
Syntax	Octet String (4)
Zugriff	lesen
Beschreibung	Liefert die Version des sog. Boot-Loaders als String. Beispiel für Version „2.65“: 0x32, 0x2e, 0x36, 0x35.

flWorkFWInfoBootState

OID	1.3.6.1.4.1.4346.11.11.11.1.7
Syntax	Octet String (6)
Zugriff	lesen
Beschreibung	Liefert das Boot-Loader-Release als String. Beispiel für „beta“: 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoBootDate

OID	1.3.6.1.4.1.4346.11.11.11.1.8
Syntax	Octet String (6)
Zugriff	lesen
Beschreibung	Liefert das Erstellungsdatum der Boot-Loader-Version als String. Beispiel für „09.03.01“: 0x30, 0x39, 0x30, 0x33, 0x30, 0x31.

flWorkFWInfoBootTime

OID	1.3.6.1.4.1.4346.11.11.11.1.9
Syntax	Octet String (6)
Zugriff	lesen
Beschreibung	Liefert die Erstellungsuhrzeit der Boot-Loader-Version als String. Beispiel für „14:10:20“: 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWInfoOperStatus

OID	1.3.6.1.4.1.4346.11.11.11.1.11
Syntax	Integer
Zugriff	lesen
Beschreibung	Liefert den Betriebszustand der Firmware: - Problem vorhanden 3 - fehlerfrei 2 - other 1

flWorkFWInfoHealthText

OID	1.3.6.1.4.1.4346.11.11.11.1.12

Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert ergänzende Informationen/Fehlerzustände der Firmware.

flWorkFWInfoDisplay

OID	1.3.6.1.4.1.4346.11.11.11.1.13
Syntax	DisplayString
Zugriff	lesen
Beschreibung	Liefert die zurzeit aktuelle Anzeige des Diagnose-Displays.

flWorkFWCtrl

OID 1.3.6.1.4.1.4346.11.11.11.2

flWorkFWCtrlBasic

OID 1.3.6.1.4.1.4346.11.11.11.2.1

flWorkFWCtrlReset

OID	1.3.6.1.4.1.4346.11.11.11.2.1.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Sie können, im Schreibzugriff, mit dem Wert „2“ einen Reset auslösen. Im Lesezugriff ist der Wert immer „1“. Nach dem Auslösen des Resets wird im Display „rb“ angezeigt.

flWorkFWCtrlHttp

OID	1.3.6.1.4.1.4346.11.11.11.2.1.6
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie den Web-Server des Switches abschalten. Die Änderung wird nach einem Neustart wirksam: Web-Server eingeschaltet 2 Web-Server ausgeschaltet 1

flWorkFWCtrlTelnet

OID	1.3.6.1.4.1.4346.11.11.11.2.1.7
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie die Telnet-Funktion des MMS abschalten. Die Änderung wird nach einem Neustart wirksam: Telnet aktiviert 2 Telnet deaktiviert 1

flWorkFWCtrlWebPageRefresh

OID	1.3.6.1.4.1.4346.11.11.11.2.1.8
Syntax	Integer (0 ... 3600)
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie die Refresh Time für die automatische Aktualisierung der Webseiten in Sekunden einstellen: Default 30 s Keine Aktualisierung 0 s

flWorkFWCtrlSNMP

OID	1.3.6.1.4.1.4346.11.11.11.2.1.9
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie den SNMP-Agenten aktvieren oder deaktivieren. Die Änderungen werden nach Neustart wirksam. SNMP-Agent deaktiviert 1 SNMP-Agent aktiviert 2

flWorkFWCtrlOperatingMode

OID	1.3.6.1.4.1.4346.11.11.11.2.1.10
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie eine Vorkonfiguration für die Betriebsart „PROFINET“ vornehmen. Standard-Modus (default) 1 PROFINET-Modus 2

flWorkFWCtrlIfCounters

OID	1.3.6.1.4.1.4346.11.11.11.2.1.11
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie die Statistik-Werte für alle Zähler von allen Ports zurückgesetzt werden. Nicht gelöscht 1 Zähler löschen 2

flWorkFWCtrlTrapDest

1.3.6.1.4.1.4346.11.11.11.2.2

flWorkFWCtrlTrapDestTable

1.3.6.1.4.1.4346.11.11.11.2.2.1

flWorkFWCtrlTrapDestEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1
Syntax	

Zugriff	
Beschreibung	Generiert eine Tabelle mit den IP-Adressen der Trap-Manager.
flWorkFWCtrlTrapDestIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Zeigt den Index der Ziel-Komponente, die die Traps empfangen soll.
flWorkFWCtrlTrapDestIPAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.2
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Zeigt die IP-Adresse der Ziel-Komponente, die die Traps empfangen soll.

flWorkFWCtrlTrapDestCapacityMax

OID	1.3.6.1.4.1.4346.11.11.11.2.2.2
Syntax	Integer32
Zugriff	lesen
Beschreibung	Nennt die maximal mögliche Anzahl der Trap-Receiver.

flWorkFWCtrlTrapDestEnable

OID	1.3.6.1.4.1.4346.11.11.11.2.2.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann das Versenden von SNMP-Traps verhindert werden: Versenden erlaubt 2 Versenden nicht erlaubt 1

flWorkFWCtrlTrapLink

OID	1.3.6.1.4.1.4346.11.11.11.2.2.4
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann eingestellt werden, dass der Trap „LinkUp/Down“ als Ergänzung die physikalische Port-Nummer hat: Ohne Ergänzung 2 Mit Ergänzung 1

flWorkFWCtrlTrapConnectionTest

OID	1.3.6.1.4.1.4346.11.11.11.2.2.5

Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Test-Traps zum Verbindungstest durch den SNMP-Agenten verschickt werden. Versenden von Test-Traps 2 Keine Test-Traps 1

flWorkFWCtrlTrapEnableTable

1.3.6.1.4.1.4346.11.11.11.2.2.10

flWorkFWCtrlTrapEnableEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1
Syntax	
Zugriff	
Beschreibung	Generiert eine Tabelle mit Informationen zu den Traps.
flWorkFWCtrlTrapEnableIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.1
Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt identifiziert den Trap durch die Trap-ID.
flWorkFWCtrlTrapEnableOid	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.2
Syntax	Object Identifier
Zugriff	lesen
Beschreibung	Zeigt die OID des Traps.
flWorkFWCtrlTrapEnableName	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.3
Syntax	Display String
Zugriff	lesen
Beschreibung	Dieses Objekt identifiziert den Trap durch den Trap-Namen.
flWorkFWCtrlTrapEnableStatus	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.4
Syntax	Integer
Zugriff	lesen - schreiben
Beschreibung	Dieses Objekt zeigt den Sende-Status des Traps. Sofern das Versenden von Traps aktiviert ist, kann jeder Trap einzeln deaktiviert werden.

flWorkFWCtrlPasswd

OID 1.3.6.1.4.1.4346.11.11.11.2.3

flWorkFWCtrlPasswdSet

OID 1.3.6.1.4.1.4346.11.11.11.2.3.1

Syntax Octet String (2 ... 24)

Zugriff lesen und schreiben

Aus Sicherheitsgründen erhalten Sie im Lesezugriff immer „*****“ als Antwort.

Beschreibung Hier können Sie ein neues Passwort mit maximal 12 Zeichen vergeben. Beispiel:
- Ihr neues Passwort soll „*factory3*“ lauten.
- Zur Kontrolle müssen Sie das Passwort zweimal eingeben.
- Ihre Eingabe „*factory3factory3*“.
- Ihr Passwort für den Schreibzugriff lautet jetzt: „*factory3*“.

flWorkFWCtrlPasswdSuccess

OID 1.3.6.1.4.1.4346.11.11.11.2.3.2

Syntax Integer

Zugriff lesen

Beschreibung Hier erhalten Sie eine Meldung, ob die letzte Passwortänderung erfolgreich war:
- nicht geändert 1
- fehlgeschlagen 2
- erfolgreich 3

Die Meldungen 2 und 3 werden für ca. zehn Minuten nach dem letzten Zugriff gemeldet, danach wird wieder der Status 1 (nicht geändert) gemeldet.

flWorkFWCtrlLoginExpire

OID 1.3.6.1.4.1.4346.11.11.11.2.3.3

Syntax Integer32 (30 ... 3600)

Zugriff lesen und schreiben

Beschreibung Hier die wird Anzahl der Sekunden als Frist zwischen zwei Passwort-Eingaben festgelegt. Nach Ablauf der Frist muss, bei Bedarf, das Passwort erneut eingegeben werden.

Default 300
Bereich 30 - 3600

flWorkFWCtrlUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4

flWorkFWCtrlTftpIpAddr

OID	1.3.6.1.4.1.4346.11.11.11.2.4.2
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Hier kann die IP-Adresse des TFTP-Servers für das Firmware-Update eingestellt werden.

flWorkFWCtrlTftpFile

OID	1.3.6.1.4.1.4346.11.11.11.2.4.3
Syntax	Octet String (0 ... 64)
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Name der Firmware-Datei für den TFTP-Download eingestellt werden.

flWorkFWCtrlUpdateStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.4.4
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Status des Firmware-Updates abgefragt werden:

Update erfolgreich	1
Update nicht erfolgreich	2
Kein Update durchgeführt	3
Unbekannt	4

flWorkFWCtrlUpdateExecute

OID	1.3.6.1.4.1.4346.11.11.11.2.4.5
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Firmware-Update ausgelöst werden.

Kein Firmware-Update	1
Firmware-Update ausführen	2

Nach einem Firmware-Update ist ein Reset erforderlich, damit die neue Firmware aktiviert wird.

flWorkFWCtrlRunningUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.6
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Status des Firmware-Updates abgefragt werden:

Firmware-Update nicht gestartet	1
Firmware-Update wird durchgeführt	2
Firmware-Update erfolgreich	3
Verbindungsfehler	4
Fehlerhafter Dateiname	5
Fehler	6

flWorkFWCtrlAutoUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.7
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Firmware-Update mit anschließendem Neustart ausgelöst werden:

Kein Firmware-Update	1
Firmware-Update ausführen	2

flWorkFWCtrlConf

OID 1.3.6.1.4.1.4346.11.11.11.2.5

flWorkFWCtrlConfStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.1
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Status der aktuellen Gerätekonfiguration abgefragt werden:

Konfiguration OK - Konfiguration entspricht der gespeicherten Konfiguration	1
Konfiguration fehlerhaft - Konfiguration entspricht nicht der gespeicherten Konfiguration, d. h. nach einem Neustart könnter der Switch mit einer anderen Konfiguration starten	2
Konfiguration gespeichert	3
Konfiguration wird zurzeit gespeichert	4

flWorkFWCtrlConfSave

OID	1.3.6.1.4.1.4346.11.11.11.2.5.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann die Gerätekonfiguration gespeichert werden:

Konfiguration nicht speichern	1
Konfiguration speichern	2

flWorkFWCtrlDefaultUponDelivery

OID	1.3.6.1.4.1.4346.11.11.11.2.5.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann das Gerät auf Werkseinstellungen (siehe „Auslieferungszustand / Werkseinstellungen“ auf Seite 3-1) gesetzt werden. Außerdem wird ein Neustart ausgelöst: Nicht auf Werkseinstellungen setzen 1 Auf Werkseinstellungen setzen 2

flWorkFWCtrlConfName

OID	1.3.6.1.4.1.4346.11.11.11.2.5.4
Syntax	Octet String (0 ... 64)
Zugriff	lesen und schreiben
Beschreibung	Hier kann ein beschreibender Name für die gespeicherte Konfiguration vergeben oder gelesen werden.

flWorkFWCtrlConfSource

OID	1.3.6.1.4.1.4346.11.11.11.2.5.5
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Speicherort der geladenen Konfiguration gelesen werden. Konfiguration vom Gerät geladen 1 Steckbarer Parametrierungsspeicher 2

flWorkFWConfig

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10

flWorkFWConfigTftpIPAddr

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.2
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Hier kann die IP-Adresse des TFTP-Servers eingestellt werden.

flWorkFWConfigTftpFile

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.3
Syntax	Octet String (0 ... 64)
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Dateiname zur TFTP-Übertragung eingestellt werden.

flWorkFWConfigStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.4
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier können Informationen zur letzten TFTP-Übertragung abgerufen werden:

Übertragung OK	1
Übertragung nicht OK	2
Keine Übertragung	3
Unbekannt	4

flWorkFWConfigExecute

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.5
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Konfigurationsdaten geladen oder abgespeichert werden:

Keine Übertragung	1
Übertragung vom Server auf den Switch	2
Übertragung vom Switch auf den Server	3

Falls nach einem Konfigurations-Download die neue Konfiguration nicht durch einen Reset aktiviert wurde, wird bei einem Speichern der Konfiguration die zuvor geladene Konfiguration verworfen und stattdessen die zurzeit aktive Konfiguration des MMS gespeichert.

flWorkFWRunningConfig

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.6
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Status der Konfigurationsdaten-Übertragung abgefragt werden:

Nicht gestartet	1
Übertragung läuft	2
Übertragung erfolgreich	3
Verbindungsfehler	4
Falscher Datei-/Pfadname	5
Fehler	6

flWorkFWCtrlConfigMemoryModule (1.3.6.1.4.1.4346.11.11.11.2.5.11)

flWorkFWCtrlConfMemoryModuleStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.1
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Status des Memory-Moduls beim MMS abgefragt werden:

Memory-Modul vorhanden	1
Memory-Modul ausgelastet	2
Memory-Modul wird nicht unterstützt	3
Memory-Modul nicht vorhanden	4
Memory-Modul defekt	5

flWorkFWCtrlConfMemoryModuleClear

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann das Memory-Moduls gelöscht werden:

Nicht gelöscht	1
Memory-Modul löschen	2

flWorkFWCtrlConfMemoryModuleCompare

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann ein Konfigurationsvergleich zwischen MMS und Memory-Modul veranlasst werden:

Nicht vergleichen	1
Konfiguration vergleichen	2

flWorkFWCtrlConfMemoryModuleCompareStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.4
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann das Ergebnis des Konfigurationsvergleichs zwischen MMS und Memory-Modul abgefragt werden:

Unbekannt	1
Vergleich läuft noch	2
Konfiguration gleich	3
Konfiguration nicht gleich	4
Memory-Modul ist leer	5

flWorkFWCtrlConfigMemInfo (1.3.6.1.4.1.4346.11.11.11.2.5.11.5)

flWorkFWCtrlConfigMemConfName

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.5.1
Syntax	Octet String
Zugriff	lesen
Beschreibung	Hier kann der Konfigurationsname der im Memory-Modul abgespeicherten Konfiguration abgefragt werden.

flWorkFWCtrlConfigMemFwVersion

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.5.2
Syntax	Octet String
Zugriff	lesen
Beschreibung	Hier kann die Firmware-Version ausgelesen werden, mit der diese Konfiguration gespeichert wurde.

flWorkFWCtrlConfigMemIpAddress

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.5.3
Syntax	Octet String
Zugriff	lesen
Beschreibung	Hier kann die IP-Adresse des Gerätes ausgelesen werden, das diese Konfiguration gespeichert hat.

flWorkFWCtrlSerial

OID 1.3.6.1.4.1.4346.11.11.11.2.6

flWorkFWCtrlSerialBaud

OID	1.3.6.1.4.1.4346.11.11.11.2.6.1
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann die eingestellte Datenübertragungsrate der seriellen Schnittstelle abgefragt werden: 2400 Baud 1 9600 Baud 2 19200 Baud 3 38400 Baud 4

flWorkFWCtrlSerialDataBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.2
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt die Anzahl der Datenbits der seriellen Schnittstelle: 8 Bit 1

flWorkFWCtrlSerialStopBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.3
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt die Anzahl der Stopbits der seriellen Schnittstelle: 1 Bit 1 2 Bits 2

flWorkFWCtrlSerialParity

OID	1.3.6.1.4.1.4346.11.11.11.2.6.4
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Paritäts-Modus der seriellen Schnittstelle: Keine 1 Ungerade 2 Gerade 3

flWorkFWCtrlSerialFlowControl

OID	1.3.6.1.4.1.4346.11.11.11.2.6.5
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt die gewählte Flusssteuerung der seriellen Schnittstelle: Keine 1 Hardware 2

flWorkFWCtrlAlarmContact

OID 1.3.6.1.4.1.4346.11.11.11.2.7

flWorkFWCtrlAlarmContactEvents

OID 1.3.6.1.4.1.4346.11.11.11.2.7.1

flWorkFWCtrlAlarmContactEventPowerSupply

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann die Meldung des Ausfalls der redundanten Spannungsversorgung über den Meldekontakt eingestellt werden: Überwachung abgeschaltet 1 Überwachung eingeschaltet 2

flWorkFWCtrlAlarmContactEventLinkState

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann die Link-Down-Meldung der Ports über den Meldekontakt eingestellt werden: Überwachung abgeschaltet 1 Überwachung eingeschaltet 2

Über das Objekt „flWorkNetPortLinkMonitoring“ können Sie die Port-Überwachung für jeden Port einzeln einstellen.

flWorkFWCtrlAlarmContactEventSecurityPortBlocked

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Meldung über den Meldekontakt, wenn von einer nicht feigegebenen MAC-Adresse auf einen Port zugegriffen wird. Nicht aktiviert 1 Aktiviert 2

flWorkFWCtrlAlarmContactEventPoEFaultDetected

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.4
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Meldung über den Meldekontakt, wenn ein PoE-Fault aufgetreten ist. Meldung über Meldekontakt nicht aktiviert 1 Meldung über Meldekontakt aktiviert 2

flWorkFWCtrlAlarmContactEnable

OID	1.3.6.1.4.1.4346.11.11.11.2.7.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann die Meldung der konfigurierten Zustände über den Meldekontakt eingestellt werden: Überwachung abgeschaltet 1 Überwachung eingeschaltet 2

flWorkFWCtrlAlarmContactStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.7.3
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier kann der Zustand des Meldekontakts abgefragt werden: Meldekontakt offen 1 Meldekontakt geschlossen 2

flWorkFWCtrlAlarmContactReason

OID	1.3.6.1.4.1.4346.11.11.11.2.7.4
Syntax	Display String
Zugriff	lesen
Beschreibung	Zeigt den Grund, aus dem der Meldekontakt geöffnet wurde.

flWorkFWCtrlSecurity

OID 1.3.6.1.4.1.4346.11.11.11.2.8

flWorkFWCtrlSecurityAccess

1.3.6.1.4.1.4346.11.11.11.2.8.1

flWorkFWCtrlSecurityAccessTable

flWorkFWCtrlSecurityAccessEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.1
flWorkFWCtrlSecurityAccessIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.1.1
Syntax	Integer32
Zugriff	lesen
Beschreibung	Zeigt den Index des Eintrages im Access Table.
flWorkFWCtrlSecurityAccessAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.1.2
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Zeigt die IP-Adresse der Geräte, die Zugriffs-Rechte auf diesen Switch haben.
flWorkFWCtrlSecurityAccessDescr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.3
Syntax	Octet String (0 ... 32)
Zugriff	lesen und schreiben
Beschreibung	Zeigt eine Beschreibung des Clients mit Zugriffsrechten.
flWorkFWCtrlSecurityAccessRight	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.4
Syntax	Integer

Zugriff	lesen und schreiben
Beschreibung	Zeigt die Zugriffsrechte des jeweiligen Clients an: Nur-Lese-Recht 1 Lese-Schreib-Recht 2
flWorkFWCtrlSecurityAccessTableCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.2
Syntax	Integer32
Zugriff	lesen
Beschreibung	Nennt die maximale Anzahl der möglichen Einträge für den Zugriff auf das WBM.
flWorkFWCtrlSecurityAccessEnable	
OID	1.3.6.1.4.1.4346.11.11.11.3.1.1.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier legen Sie fest, ob der Zugriff auf das WBM über Zugriffsrechte für einzelne Clients reglementiert wird oder nicht (ist keine gültige IP-Adresse angegeben, wird automatisch „Ohne Reglement“ eingestellt): Ohne Reglement 1 Mit Reglement 2

flWorkFWCtrlSecurityPort

OID 1.3.6.1.4.1.4346.11.11.11.2.8.2

flWorkFWCtrlSecurityPortTable

flWorkFWCtrlSecurityPortEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1
flWorkFWCtrlSecurityPortIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.1
Syntax	Integer32
Zugriff	lesen
Beschreibung	Zeigt den Index des Eintrages in der Port List.
flWorkFWCtrlSecurityPortLastMacAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.2
Syntax	MacAddress
Zugriff	lesen
Beschreibung	Zeigt die letzte MAC-Adresse, von der an diesem Port Frames empfangen wurden.
flWorkFWCtrlSecurityPortMode	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.3
Syntax	Integer
Zugriff	lesen und schreiben

Beschreibung	Zeigt den Security-Modus des Ports an oder ändert ihn:	
	Kein Sicherheitsmodus aktiviert	1
	Bei unerlaubtem Zugriff nur Trap-Versand	2
	Bei unerlaubtem Zugriff Blockierung des Ports	3
	Bei unerlaubtem Zugriff Blockierung des Ports mit späterer automatischer Freigabe	4

flWorkFWCtrlSecurityPortState	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.4
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt den Security-Status des Ports an oder ändert ihn:
	Port wieder freigegeben (OK) 1 Port zurzeit blockiert 2 Port zurzeit blockiert, wird später automatisch freigegeben 3
	Falls weiterhin Pakete von illegalen MAC-Adressen empfangen werden, schaltet der Port sofort wieder in einen der blockierenden Modi um.

flWorkFWCtrlSecurityPortIllegalAddrCounter	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.5
Syntax	Gauge32
Zugriff	lesen
Beschreibung	Nennt die Anzahl der nicht zugelassenen MAC-Adressen, die an diesem Port registriert wurden.

flWorkFWCtrlSecurityPortMacTable

flWorkFWCtrlSecurityPortMacEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1
flWorkFWCtrlSecurityPortMacIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1.1
Syntax	Integer32
Zugriff	lesen
Beschreibung	Zeigt die Port-Nummer.
flWorkFWCtrlSecurityPortMacAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1.2
Syntax	MacAddress
Zugriff	lesen und schreiben
Beschreibung	Zeigt die zugelassenen MAC-Adressen für diesen Port.
flWorkFWCtrlSecurityPortMacDescr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1.3
Syntax	Octet String (0 ... 16)
Zugriff	lesen und schreiben
Beschreibung	Zeigt eine Anwender-Beschreibung der MAC-Adresse.

flWorkFWCtrlSecurityPort

flWorkFWCtrlSecurityPortTableCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.3
Syntax	Integer32
Zugriff	lesen
Beschreibung	Nennt die Anzahl der maximal möglichen Einträge in der Security-Port-Tabelle.
flWorkFWCtrlSecurityPortMacTableCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.4
Syntax	Integer32
Zugriff	lesen
Beschreibung	Zeigt die maximal mögliche Anzahl der zugelassenen MAC-Adressen je Port an.
flWorkFWCtrlSecurityPortEnable	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.5
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt, ob der Sicherheitsmechanismus für diesen Port aktiv ist. Falls keine gültige MAC-Adresse definiert wurde, ist der Mechanismus deaktiviert. Mechanismus deaktiviert 1 Mechanismus aktiviert 2
flWorkFWCtrlSecurityPortIllegalAddrCounterClear	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.6
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Löscht alle Zähler der nicht zugelassenen Adressen. Beim Lesezugriff wird immer (1 - nicht gelöscht) übertragen. Nicht gelöscht 1 Löschen 2

flWorkFWCtrlProfinet

flWorkFWCtrlProfinetAlarm

flWorkFWCtrlProfinetAlarmPortTable

flWorkFWCtrlProfinetAlarmPortEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1
flWorkFWCtrlProfinetAlarmPortIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Zeigt die Port-Nummer.
flWorkFWCtrlProfinetAlarmPortLinkMonitoring	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.2

Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Im PROFINET-Modus kann ein Slot einen Alarm senden, wenn sich der Link-Status von „Verbunden“ auf „Nicht verbunden“ ändert: Kein Alarm abschicken 1 Alarm abschicken 2

flWorkFWCtrlProfinetAlarmPortPofScrjDiag	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Im PROFINET-Modus kann ein Slot einen Alarm senden, wenn die Empfangsleistung eines POF-SCRJ-Ports einen kritischen Wert erreicht oder der Port in einen kritischen Zustand fällt: Kein Alarm abschicken 1 Alarm abschicken 2

flWorkFWCtrlProfinetAlarmPowerSupply	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.10
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Im PROFINET-Modus kann der Switch einen Alarm senden, wenn eine der redundanten Spannungsversorgungen ausfällt: Kein Alarm abschicken 1 Alarm abschicken 2

flWorkFWCtrlProfinetAlarmModuleRemove	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.11
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Im PROFINET-Modus kann der Switch einen Alarm senden, wenn eines der Interface-Module entfernt wird: Kein Alarm abschicken 1 Alarm abschicken 2

flWorkFWCtrlMRP

flWorkFWCtrlMRPConfig

flWorkFWCtrlMRPConfigDomainTable

flWorkFWCtrlMRPConfigDomainEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1

flWorkFWCtrlMRPConfigDomainIdx	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Zeigt den Index des Eintrags.

flWorkFWCtrlMRPConfigDomainUdid	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.2
Syntax	Octet String
Zugriff	lesen und schreiben
Beschreibung	In der IEC 61158-5-10 ist die Struktur der UUID als numerische ID festgelegt.
flWorkFWCtrlMRPConfigDomainName	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.3
Syntax	Octet String
Zugriff	lesen und schreiben
Beschreibung	Enthält einen beschreibenden Namen für diesen MRP-Ring (Default: MRP-Domain)
flWorkFWCtrlMRPConfigDomainRole	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.4
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können die möglichen MRP-Betriebsarten eingestellt werden: Kein MRP-Betrieb 0 MRP-Betrieb als Client 1 MRP-Betrieb als Manager 2 Betriebsart löschen 3 Betriebsart setzen 4
flWorkFWCtrlMRPConfigDomainManagerPriority	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.5
Syntax	Integer (0 ... 65535)
Zugriff	lesen und schreiben
Beschreibung	Priorität dieses MRP-Teilnehmers, sofern es MRP-Manager ist. Wird ignoriert, wenn das Gerät MRP-Client ist. Nur die vier höchstwertigen Bits benutzen, die Bits 11-0 sind reserviert. Je niedriger der Wert, um so höher die Priorität (Default: 32768).
flWorkFWCtrlMRPConfigDomainVlanID	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.6
Syntax	Integer (0 ... 4094)
Zugriff	lesen und schreiben
Beschreibung	Hier wird die VLAN-ID festgelegt.
flWorkFWCtrlMRPConfigDomainRingPort1	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.7
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Legt den ersten MRP-Ring-Port dieses Switches fest.
flWorkFWCtrlMRPConfigDomainRingPort2	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.8
Syntax	Integer
Zugriff	lesen und schreiben

Beschreibung	Legt den zweiten MRP-Ring-Port dieses Switches fest.
flWorkFWCtrlMRPConfigDomainResetRoundTripDelays	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.9
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Löscht die Min-/Max-Werte des Round Trip Delays.

flWorkFWCtrlMRPInfo

flWorkFWCtrlMRPInfoDomainTable

flWorkFWCtrlMRPInfoDomainEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1
flWorkFWCtrlMRPInfoDomainIdx	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.1
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Index der MRP-Domäne.
flWorkFWCtrlMRPInfoDomainUdid	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.2
Syntax	Octet String
Zugriff	lesen
Beschreibung	In der IEC 61158-5-10 ist die Struktur der UUID als numerische ID festgelegt.
flWorkFWCtrlMRPInfoDomainName	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.3
Syntax	Octet String
Zugriff	lesen
Beschreibung	Enthält einen beschreibenden Namen für diesen MRP-Ring (Default: MRP-Domain)
flWorkFWCtrlMRPInfoDomainRole	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.4
Syntax	Integer
Zugriff	lesen
Beschreibung	Hier können die möglichen MRP-Betriebsarten ausgelesen werden: Kein MRP-Betrieb 0 MRP-Betrieb als Client 1 MRP-Betrieb als Manager 2
flWorkFWCtrlMRPInfoDomainManagerPriority	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.5
Syntax	Integer (0 ... 65535)
Zugriff	lesen
Beschreibung	Zeigt die Priorität dieses MRP-Teilnehmers, sofern es MRP-Manager ist.
flWorkFWCtrlMRPInfoDomainRingPort1	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.7

Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt den ifIndex des ersten MRP-Ring-Ports dieses Switches.
flWorkFWCtrlMRPInfoDomainRingPort1State	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.8
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Status des ersten MRP-Ring-Ports dieses Switches: Abgeschaltet 1 Blocking 2 Forwarding 3
flWorkFWCtrlMRPInfoDomainRingPort2	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.9
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt den ifIndex des zweiten MRP-Ring-Ports dieses Switches.
flWorkFWCtrlMRPInfoDomainRingPort2State	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.10
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Status des zweiten MRP-Ring-Ports dieses Switches: Abgeschaltet 1 Blocking 2 Forwarding 3
flWorkFWCtrlMRPInfoDomainState	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.2.1.1.11
Syntax	Integer
Zugriff	lesen
Beschreibung	Nennt den operativen Zustand dieses MRP-Ringes. MRP deaktiviert 0 Client 1 MRP-Ring geschlossen 2 MRP-Ring offen 3
flWorkFWCtrlMRPInfoDomainError	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.12
Syntax	Integer
Zugriff	lesen
Beschreibung	Nennt den Grund, aus dem sich dieses Gerät nicht in den gewünschten Zustand schalten lässt: Operativer und administrativer Zustand sind gleich (kein Fehler) 0 Ungültig, da Client 1 Mehrere MRP-Manager im Ring 2 MRP-Test-Frames erreichen nur einen MRP-Ring-Port 4

flWorkFWCtrlMRPInfoDomainRingOpenCount	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.13
Syntax	Integer
Zugriff	lesen
Beschreibung	Zähler für MRP-Ring-Port-Änderungen (nur beim Manager).
flWorkFWCtrlMRPInfoDomainLastRingOpenChange	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.14
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt den Zeitpunkt seit der letzten MRP-Ring-Port-Status-Änderung an.
flWorkFWCtrlMRPInfoDomainRoundTripDelayMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.15
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt die Zeit des maximalen Round-Trip-Delays seit dem Gerätestart in Millisekunden an.
flWorkFWCtrlMRPInfoDomainRoundTripDelayMin	
OID	1.3.6.1.4.1.4346.11.11.11.2.10.1.1.1.16
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt die Zeit des minimalen Round-Trip-Delays seit dem Gerätestart in Millisekunden an.

flWorkFWCtrlMRPInfoDeviceBlockingSupport

OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.2.2	
Syntax	Integer32	
Zugriff	lesen	
Beschreibung	Zeigt, ob der der Port „Blocking“ unterstützt.	
	Unterstützt „Blocking“ nicht	1
	Unterstützt „Blocking“	2

flSwitch

OID 1.3.6.1.4.1.4346.11.11.15

flSwitchCtrl

OID 1.3.6.1.4.1.4346.11.11.15.1

flSwitchCtrlSpanTree

OID	1.3.6.1.4.1.4346.11.11.15.1.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Aktiviert/deaktiviert STP für den Switch.

STP deaktiviert 1
STP aktiviert 2

Um STP aktivieren zu können, muss das Objekt „flSwitchCtrlRedundancy“ auf STP eingestellt werden.

flSwitchCtrlRedundancy

OID	1.3.6.1.4.1.4346.11.11.15.1.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt den gewählten Redundanz-Mechanismus für den Switch. Falls „Keine Redundanz“ ausgewählt wird, werden alle Redundanz-Mechanismen und die zugehörigen Web-Seiten abgeschaltet. Ist RSTP aktiviert, werden die Web-Seiten für RSTP freigeschaltet.

Keine Redundanz 1
RSTP aktiviert 2

Zur Konfiguration von STP wird die Bridge_MIB genutzt, siehe Seite 4-60.

flSwitchCtrlMulticast

OID	1.3.6.1.4.1.4346.11.11.15.1.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt, ob die zur Einstellung von Multicast-Betrieb notwendigen Web-Seiten angezeigt werden.

Web-Seiten ausblenden 1
Web-Seiten einblenden 2

flSwitchCtrlVLAN

OID	1.3.6.1.4.1.4346.11.11.15.1.4
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Zeigt, ob die zur VLAN-Konfiguration notwendigen Web-Seiten freigeschaltet sind. VLAN-Web-Seiten ausgeblendet 1 VLAN-Web-Seiten eingeblendet 2

flSwitchCtrlVLANTagMode

OID	1.3.6.1.4.1.4346.11.11.15.1.5
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Im Modus „Transparent“ ignoriert der Switch die VLAN-ID und richtet sich bei der Weiterleitung nur nach der Priorität. Im Modus „Tagging“ werden die Pakete gemäß der Regelung weitergeleitet. Transparent 1 Tagging 2

flSwitchCtrlVLANTagStatus

OID	1.3.6.1.4.1.4346.11.11.15.1.6
Syntax	Integer
Zugriff	lesen
Beschreibung	Zeigt, in welchem VLAN-Modus sich der Switch befindet: Transparent 1 Tagging 2

flSwitchCtrlLldp

OID	1.3.6.1.4.1.4346.11.11.15.1.7
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie das LLDP (Link Layer Discovery Protocol) ein-/ausschalten: LLDP deaktiviert 1 LLDP aktiviert 2 Senden 3 Empfangen 4

flSwitchCtrlRSTPLargeTreeSupport

OID	1.3.6.1.4.1.4346.11.11.15.1.8
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie im RSTP-Large-Tree-Modus die Anzahl der Switches, die unterhalb der Root angeschlossen werden können, von sieben auf 28 Switches erhöhen: Bis zu sieben Switches unterhalb der Root 1 Bis zu 28 Switches unterhalb der Root 2

flSwitchCtrlHashMode

OID	1.3.6.1.4.1.4346.11.11.15.1.9
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie die Suchmethode des Switches im MAC Address Table einstellen: Optimierte Suchmethode für willkürlich abgelegte MAC-Adressen (Default) 1 Optimierte Suchmethode für aufsteigend abgelegte MAC-Adressen 2

flSwitchCtrlDhcpRelayAgentUi

OID	1.3.6.1.4.1.4346.11.11.15.1.10
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie die Konfigurationsseite des DHCP Relay Agenten im WBM einblenden oder ausblenden: DHCP Relay Agent-Konfigurationsseite ausblenden 1 DHCP Relay Agent-Konfigurationsseite einblenden (Default) 2

flSwitchCtrlMacTableErase

OID	1.3.6.1.4.1.4346.11.11.15.1.11
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie veranlassen, dass der Switch alle Einträge seiner MAC-Adresstabelle löscht: MAC-Adresstabelle nicht löschen 1 MAC-Adresstabelle löschen 2

flSwitchPortMirr

OID	1.3.6.1.4.1.4346.11.11.11.15.2

flSwitchPortMirrDestinationPort

OID	1.3.6.1.4.1.4346.11.11.11.15.2.1
Syntax	Integer32
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Port (Ziel-Port), der die Daten eines anderen Ports (Quell-Port) spiegelt, eingestellt werden: Kein Port-Mirroring 0

flSwitchPortMirrSourcePort

OID	1.3.6.1.4.1.4346.11.11.11.15.2.2
Syntax	Integer32
Zugriff	lesen und schreiben
Beschreibung	Hier kann der Port (Quell-Port), dessen Daten auf einen anderen Port (Ziel-Port) gespiegelt werden, eingestellt werden: Kein Port-Mirroring 0

flSwitchPortMirrStatus

OID	1.3.6.1.4.1.4346.11.11.11.15.2.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann Port-Mirroring ein-/ausgeschaltet werden: Kein Port-Mirroring: 1 Port-Mirroring eingeschaltet 2

Das Port-Mirroring wird abgeschaltet, wenn eines oder beide der Objekte „**flSwitchPortMirrDestinationPort“** / „**flSwitchPortMirrSourcePort**“ den Wert „Null“ oder gleiche Werte (z. B. beide 2) haben.

flSwitchIgmp

OID 1.3.6.1.4.1.4346.11.11.15.3

flSwitchIgmpSnoop

OID 1.3.6.1.4.1.4346.11.11.15.3.1

flSwitchIgmpSnoopEnable

OID	1.3.6.1.4.1.4346.11.11.15.3.1.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier kann die IGMP-Snooping-Funktion aktiviert werden: Deaktiviert 1 Aktiviert 2

flSwitchIgmpSnoopAging

OID	1.3.6.1.4.1.4346.11.11.15.3.1.3
Syntax	Integer (30 ... 3600)
Zugriff	lesen und schreiben
Beschreibung	Hier kann die Dauer der Timeout-Periode der dynamisch per IGMP-Snooping gelernten Multicast-Gruppen in Sekunden eingegeben werden.

flSwitchIgmpSnoopTable

OID	1.3.6.1.4.1.4346.11.11.15.3.1.4

flSwitchIgmpSnoopEntry

OID	1.3.6.1.4.1.4346.11.11.15.3.1.4.1

flSwitchIgmpSnoopEgressPorts

OID	1.3.6.1.4.1.4346.11.11.15.3.1.4.1.1
Syntax	PortList
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt die Ports, die aufgrund von IGMP-Snooping Multicast-Daten weiterleiten.

flSwitchIgmpSnoopExtended

flSwitchBlockUnknownMulticastAtQuerier

OID	1.3.6.1.4.1.4346.11.11.15.3.1.5.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Ist die Funktion aktiviert, leitet der Switch nur dann Multicast-Pakete weiter, von denen er zuvor Membership Reports erhalten hat.

Aktiviert	2
Deaktiviert	1

flSwitchForwardUnknownMulticastToQuerier

OID	1.3.6.1.4.1.4346.11.11.15.3.1.5.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	

flSwitchIgmpQuery

OID 1.3.6.1.4.1.4346.11.11.15.3.2

flSwitchIgmpQueryTable

OID 1.3.6.1.4.1.4346.11.11.15.3.2.1

flSwitchIgmpQueryEntry

1.3.6.1.4.1.4346.11.11.15.3.2.1.1

flSwitchIgmpQueryPorts

OID	1.3.6.1.4.1.4346.11.11.15.3.2.1.1.1
Syntax	Portlist
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt die Ports, die IGMP-Router-Query-BPDUs empfangen haben.

flSwitchIgmpQueryEnable

OID	1.3.6.1.4.1.4346.11.11.15.3.2.2
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Über dieses Objekt legen Sie fest, nach welcher Protokoll-Version der Switch IGMP-Query versendet. Deaktiviert: 1 Version 1: 2 Version 2: 3

flSwitchIgmpQueryInterval

OID	1.3.6.1.4.1.4346.11.11.15.3.2.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Über dieses Objekt legen Sie fest, in welchem Zeitintervall der Switch IGMP-Queries versendet. Default: 125 s Zulässiger Wertebereich: 10 s bis 3600 s (in Schritten von 1 s)

flSwitchIgmpTableErase

OID	1.3.6.1.4.1.4346.11.11.15.3.3
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie veranlassen, dass der Switch alle Einträge seiner IGMP-Tabelle löscht: IGMP-Tabelle nicht löschen 1 IGMP-Tabelle löschen 2

flSwitchRedundancy

OID	1.3.6.1.4.1.4346.11.11.15.4

flSwitchCtrlRSTPFastRingDetection

OID	1.3.6.1.4.1.4346.11.11.15.4.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Mit diesem Objekt können Sie einstellen, ob Sie den Standard-RSTP oder zusätzlich die Fast-Ring-Detection nutzen wollen: Standard-RSTP 1 Fast-Ring-Detection 2

flSwitchRSTPRingTable

OID	1.3.6.1.4.1.4346.11.11.15.4.2
	flSwitchRSTPRingEntry
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1
	flSwitchRSTPRingIndex
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.1
Syntax	Integer (1 ... 1024)
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die Nummer des RSTP-Rings
flSwitchRSTPRingMAC	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.2
Syntax	MacAddress
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die MAC-Adresse des Switches, der den alternativen Port/Pfad in diesem Ring bildet.
flSwitchRSTPRingBlockPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.3
Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die Nummer des geblockten Ports in diesem Ring.
flSwitchRSTPRingRootPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.4
Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die Nummer des lokalen Ports (oft der Root-Port) in diesem Ring.
flSwitchRSTPRingDesPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.5

Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die Nummer eines lokalen Ports (Designated Port) in diesem Ring.
flSwitchRSTPRingStatus	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.6
Syntax	Integer
Zugriff	lesen
Beschreibung	Dieses Objekt nennt den Status des RSTP-Rings: Ring geschlossen 3 Ring nicht geschlossen 6 Fehler 7
flSwitchRSTPRingFailedPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.3
Syntax	Integer32
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die Nummer des fehlerhaften Ports im Ring.

flSwitchRelayAgentDHCP

OID 1.3.6.1.4.1.4346.11.11.15.5

flSwitchRelayAgentDhcpCtrl

OID	1.3.6.1.4.1.4346.11.11.15.5.1
Syntax	Integer
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie den Status des DHCP Relay Agents einstellen: DHCP Relay Agent deaktiviert 1 DHCP Relay Agent aktiviert 2

Wenn für die Vergabe der IP-Parameter DHCP aktiviert ist, wird der DHCP Relay Agent automatisch deaktiviert.

flSwitchRelayAgentDhcpIpAddress

OID	1.3.6.1.4.1.4346.11.11.15.5.2
Syntax	IpAddress
Zugriff	lesen und schreiben
Beschreibung	Hier können Sie die IP-Adresse des DHCP-Servers für den DHCP Relay Agent einstellen (Default 0).

	flSwitchRelayAgentDhcpStatus
OID	1.3.6.1.4.1.4346.11.11.15.5.3
Syntax	Octet String (1 ... 255)
Zugriff	lesen
Beschreibung	Dieses Objekt zeigt den Status des DHCP Relay Agents. Der Status wird beeinflusst durch: – das Objekt „flSwitchRelayAgentDhcpCtrl“ und – durch den Vergabemechanismus für die IP-Parameter
	flSwitchRelayAgentDhcpRIdType
OID	1.3.6.1.4.1.4346.11.11.15.5.4
Syntax	Integer (ipAddress (1), macAddress (2))
Zugriff	lesen und schreiben
Beschreibung	Dieses Objekt zeigt, ob der DHCP Relay Agent als Remote-ID seine MAC-Adresse oder seine IP-Adresse angibt, wenn er die Felder für die DHCP Option 82 einfügt (Default: IP-Adresse).
	flSwitchRelayAgentDhcpPortTable
OID	1.3.6.1.4.1.4346.11.11.15.5.5
	flSwitchRelayAgentDhcpPortEntry

OID	1.3.6.1.4.1.4346.11.11.15.5.5.1
Syntax	
Zugriff	
Beschreibung	Diese Tabelle zeigt die portbezogenen Informationen des DHCP Relay Agenten
flSwitchRelayAgentDhcpPortCtrlIndex	
OID	1.3.6.1.4.1.4346.11.11.15.5.5.1.1
Syntax	Integer32 (1 ... 1024)
Zugriff	lesen
Beschreibung	Dieses Objekt nennt die Port-Nummer.
flSwitchRelayAgentDhcpPortCtrlOperation	
OID	1.3.6.1.4.1.4346.11.11.15.5.5.1.2
Syntax	Integer32
Zugriff	lesen - schreiben
Beschreibung	Hier kann der DHCP Relay Agent an diesem Port aktiviert oder deaktiviert werden: DHCP Relay Agent an diesem Port deaktiviert: 1 DHCP Relay Agent an diesem Port aktiviert: 2

4.4 Management über lokale V.24-Kommunikationsschnittstelle

4.4.1 Allgemeine Funktion

Über die V.24-Schnittstelle im Mini-DIN-Format kann eine lokale Kommunikationsverbindung mit einer externen Management-Station aufgebaut werden. Verwenden Sie das Programmierkabel „PRG CAB MINI DIN“ (Art-Nr. 2730611). Die Kommunikations-Verbindung wird über eine entsprechende Emulation zwischen dem Switch und einem PC (z. B. Hyperterminal unter Windows) hergestellt und ermöglicht den Zugriff auf das User Interface.

Die Bezugspotenziale der V.24-Schnittstelle und der Versorgungsspannung sind nicht potenzialgetrennt.

4.4.1.1 Konfiguration der Schnittstelle

Nehmen Sie die nachfolgend gezeigten Einstellung an Ihrem Windows-PC vor.

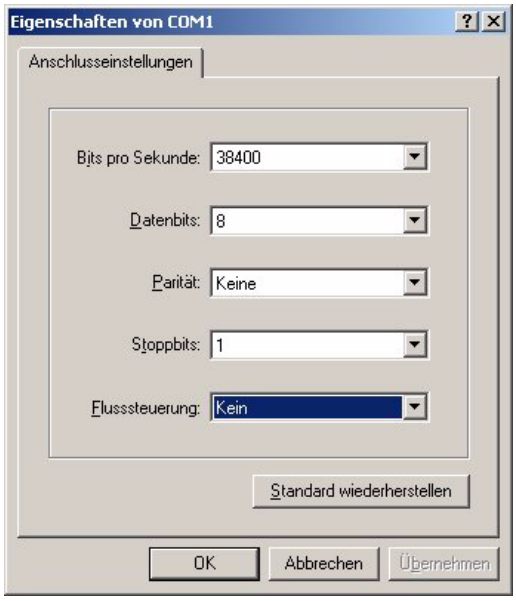


Bild 4-50 Konfiguration des Hyperterminals

4.4.1.2 Aufruf des User Interfaces

Verbinden Sie den PC und den Switch durch ein geeignetes Kabel (PRG CAB MINI DIN, Art-Nr. 2730611) miteinander. Drücken Sie nach Herstellung der Verbindung die Tastenkombination Ctrl + L des PCs. Der Bildschirminhalt wird daraufhin vom Switch angefordert.

4.4.2 Funktionen des User Interfaces

4.4.2.1 Funktion während des Boot-Vorgangs nach Neustart

Wenn Sie direkt nach dem Neustart des MMS in den ersten fünf Sekunden das User-Interface öffnen, haben Sie die Möglichkeit ein Firmware-Update auszulösen. Da zu diesem frühen Zeitpunkt die eigentliche Switch-Firmware noch nicht gestartet ist, kann selbst im Fehlerfall, z. B. wenn sich eine defekte Firmware auf dem Gerät befindet, diese Firmware noch aktualisiert werden (siehe Kapitel „Start mit defekter Software (Firmware)“ auf Seite 4-125).

4.4.2.2 Funktionen während des Betriebs

Im User-Interface stehen Ihnen folgende Funktionen zur Verfügung:

– Einstellung der IP-Parameter
– Auswahl des Adressierungsmechanismus
– Rücksetzen auf Werkseinstellungen
– Aktivierung/Deaktivierung des Webservers, der Telnet-Funktion und SNMP
– Aktivierung/Deaktivierung von Port-Security, Access Control for Web
– Umschalten des VLAN-Modes
– Umschalten des Operating-Modes
– Aktivierung/Deaktivierung des Redundanz-Mechanismus RSTP
– Reset

Die Aktivierung/Deaktivierung des Webservers oder der Telnet-Funktion ist erst nach einem „SAVE“ und einem anschließenden Neustart wirksam.

Vorgenommene Einstellungen werden mit „APPLY“ nur übernommen, aber **nicht** dauerhaft gespeichert. Eine dauerhafte Speicherung der jetzigen Konfigurationseinstellungen erreichen Sie mit „SAVE“.

4.4.2.3 Aufbau der Seiten des User-Interfaces

Login Screen

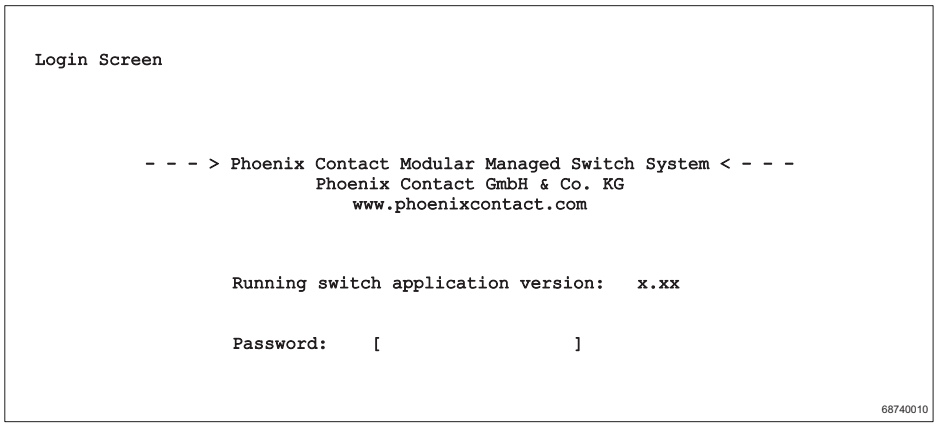

Login Screen
- - - > Phoenix Contact Modular Managed Switch System < - - -
Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
Running switch application version: x.xx
Password: [ ]
68740010

Bild 4-51 Startseite des User-Interfaces

Auf der Startseite erfahren Sie die Version der verwendeten Firmware. Für weitere Einstellungen ist die Eingabe des Passwortes erforderlich. Im Auslieferungszustand lautet das Passwort „private“. Beachten Sie dabei die Groß-/Kleinschreibung. Es wird dringend empfohlen, das Passwort zu ändern (über SNMP oder WBM).

Basic Switch Configuration

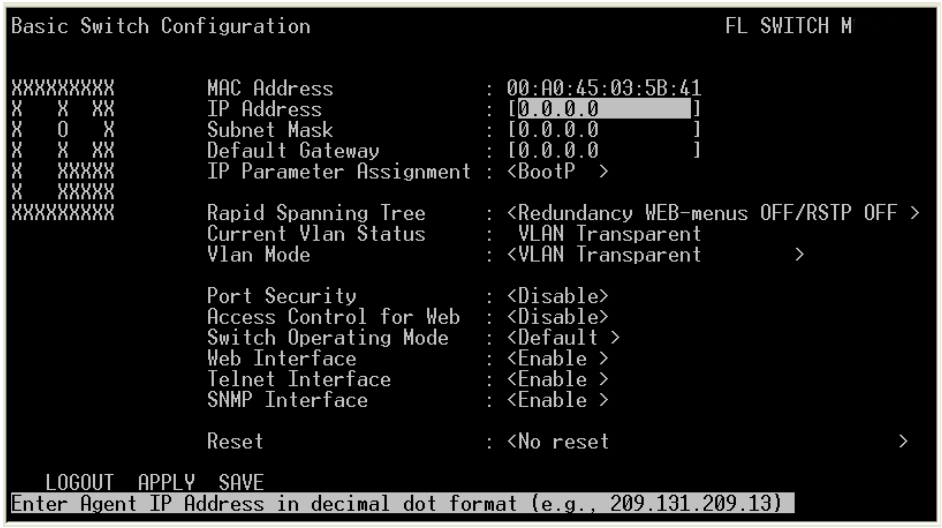


Bild 4-52 IP-Konfiguration im User-Interface

Neben der Anzeige der fest eingestellten MAC-Adresse haben Sie hier die Möglichkeit, die IP-Parameter auszulesen oder zu verändern.

Um die IP-Parameter einstellen zu können, muss bei „IP Parameter Assignment“ die Option „Static“ gewählt sein.

Auf dieser Seite des User-Interfaces bestimmen Sie den Adressierungsmechanismus oder lösen einen Neustart des Gerätes aus.

Vorgenommene Einstellungen werden mit „APPLY“ nur übernommen, aber **nicht** dauerhaft gespeichert. Eine dauerhafte Speicherung der jetzigen Konfigurationseinstellungen erreichen Sie mit „SAVE“.

Rücksetzen auf Werkseinstellungen

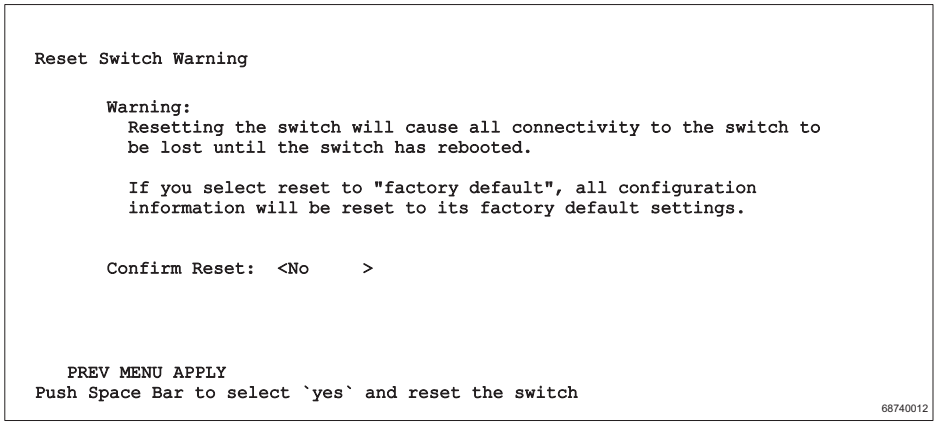

Reset Switch Warning
Warning:
Resetting the switch will cause all connectivity to the switch to be lost until the switch has rebooted.
If you select reset to "factory default", all configuration information will be reset to its factory default settings.
Confirm Reset: <No >
PREV MENU APPLY
Push Space Bar to select `yes` and reset the switch
68740012

Bild 4-53 Rücksetzen auf Werkseinstellungen

Auf dieser Seite haben Sie die Möglichkeit, den Switch auf Werkseinstellungen zurück zu setzen oder neu zu starten. Sie erreichen diese Seite, indem Sie auf der Seite „Basic Switch Configuration“ die Option „Reset“ auf „Reset Switch“ oder „Reset Switch to factory defaults“ setzen und dann „Apply“ oder „Save“ wählen. Jede Konfigurationsänderung wird rückgängig gemacht, alle IP-Parameter werden in den Auslieferungszustand (siehe Kapitel 3.1.1 auf Seite 3-1) zurückgesetzt.

Das Rücksetzen auf Werkseinstellungen setzt auch das Passwort auf „private“ zurück. Aus Sicherheitsgründen wird die Änderung auf ein neues, nur Ihnen bekanntes Passwort empfohlen.

4.4.3 Start mit defekter Software (Firmware)

Falls die Software (Firmware), die auf dem MMS installiert ist, defekt ist, haben Sie dennoch die Möglichkeit, die Firmware durch ein Update wieder herzustellen oder zu aktualisieren. Beachten Sie auch die 7-Segment-Anzeige (siehe auch Seite 1-15).

Vorgehen:

– Verbinden Sie den Switch über die serielle V.24-Schnittstelle mit Ihrem PC. Stellen Sie sicher, dass Ihr Hyperterminal korrekt konfiguriert ist (siehe Konfiguration auf Seite 4-121)
– Starten Sie den Switch neu.

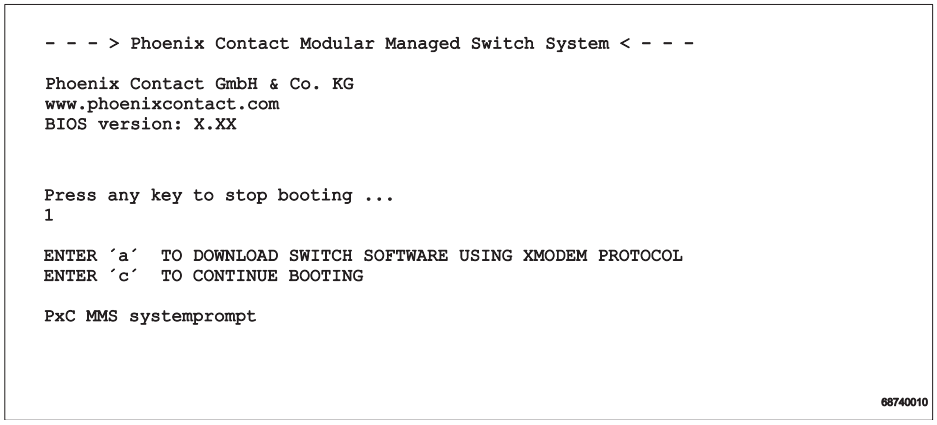

- - - > Phoenix Contact Modular Managed Switch System < - - -
Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
BIOS version: X.XX
Press any key to stop booting ...
1
ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING
PxC MMS systemprompt
68740010

Bild 4-54 Bildschirmansicht über Hyperterminal während des Bootens

Falls die Firmware des Gerätes defekt ist, erscheint jetzt folgende Ansicht:

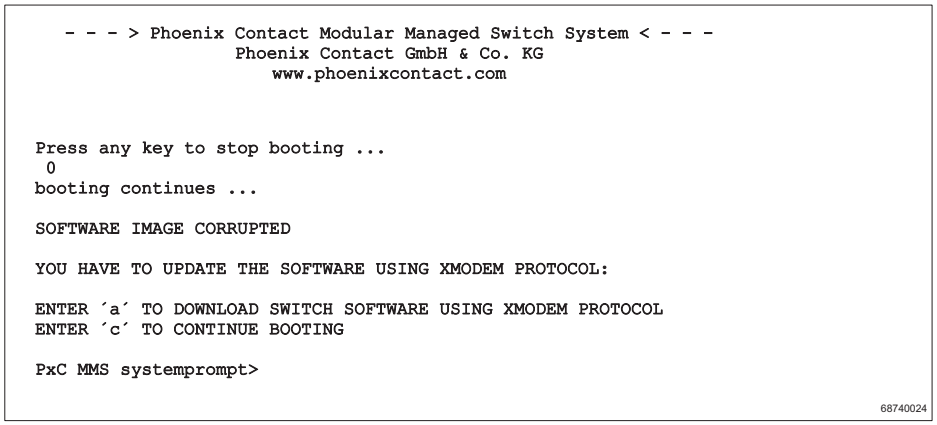

- - - > Phoenix Contact Modular Managed Switch System < - - -
Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
Press any key to stop booting ...
0
booting continues ...
SOFTWARE IMAGE CORRUPTED
YOU HAVE TO UPDATE THE SOFTWARE USING XMODEM PROTOCOL:
ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING
PxC MMS systemprompt>
68740024

Bild 4-55 Auswahl-Menü bei defekter Firmware

Nachdem mit „a“ der Download der neuen Software ausgelöst wurde, erscheint:

```
   - - - > Phoenix Contact Modular Managed Switch System < - - -
                  Phoenix Contact GmbH & Co. KG
                     www.phoenixcontact.com



ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC MMS systemprompt> a

Downloading firmware image with XMODEM over serial port ...

XMODEM Receive: Waiting for Sender ...

-_
```

68740025

Bild 4-56 XMODEM-Bereitschaft

Jetzt erwartet der Switch die neue Firmware. Wählen Sie im Hyperterminal aus dem Menü „Übertragung“ jetzt „Datei senden“ aus.

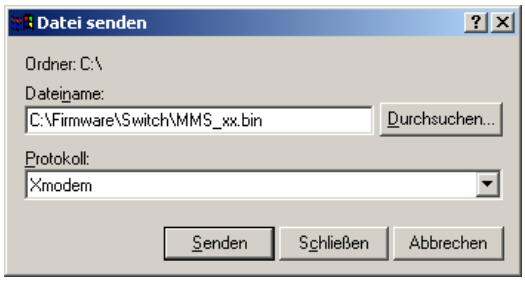


Bild 4-57 Xmodem - Datei senden

Achten Sie darauf, dass als Protokoll „Xmodem“ eingestellt ist. Anderenfalls schlägt die Übertragung fehl.

Nach dem Klicken auf „Senden“ wird die Datei übertragen. In der nachfolgenden Ansicht können Sie den Fortschritt der Dateiübertragung verfolgen.

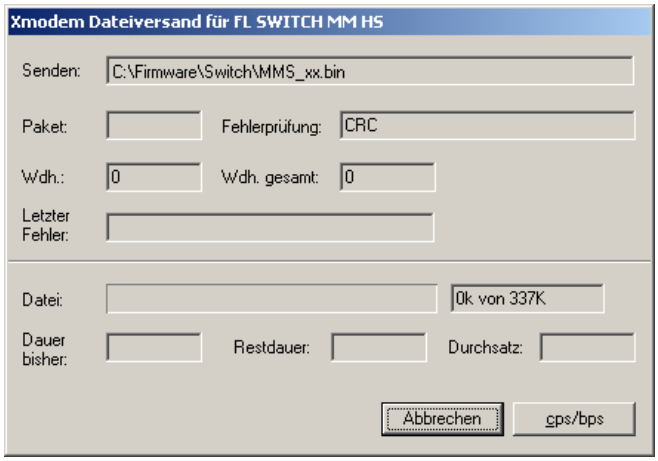


Bild 4-58 Dateiübertragung mit Xmodem

Die Dateiübertragung kann einige Minuten dauern. Unternehmen Sie keine weiteren Schritte, solange die Box angezeigt wird.

Nachdem die Box nicht mehr angezeigt wird, erscheint im Hyperterminal eine Erfolgsmeldung. Führen Sie jetzt mit „c“ den Bootvorgang fort oder lösen Sie jetzt mit dem Reset-Taster einen Reset aus.

4.5 Management über Telnet

Das Telnet-Protokoll stellt die Funktion eines virtuellen Terminals zur Verfügung. Es ermöglicht den Fernzugriff vom eigenen Computer auf andere im Netzwerk befindliche Systeme (z. B. PCs oder MMS). Telnet setzt auf TCP/IP über das Netzwerk auf, unterstützt die Funktionen der Schichten 5 bis 7 und ermöglicht eine bidirektionale Kommunikation, um Datenendgeräte mit entsprechenden Prozessen zu verbinden. Das Zielsystem wird dabei allgemein als Telnet-Server bezeichnet, das eigene lokale System als Telnet-Client. Die Verbindung ist nur zwischen Telnet-Client und Telnet-Server möglich. Dem Client erscheint der Telnet-Server wie ein lokal angeschlossenes Terminal.

4.5.1 Konfiguration des Telnet-Terminals

Damit eine Telnet-Verbindung zwischen dem PC und dem MMS aufgebaut werden kann, müssen die IP-Parameter der beiden Teilnehmer so aufeinander abgestimmt sein, dass sie sich im gleichen Subnetz befinden.

Aufruf/Aufbau der Telnet-Verbindung

Verbinden Sie den PC und den Switch zu/mit einem Ethernet-Netzwerk. Wählen Sie aus dem Start-Menü die Option „Ausführen“. Tragen Sie den nachfolgenden Befehl und die IP-Adresse des MMS ein. Durch Drücken der OK-Taste wird die Verbindung zum Switch aufgebaut.

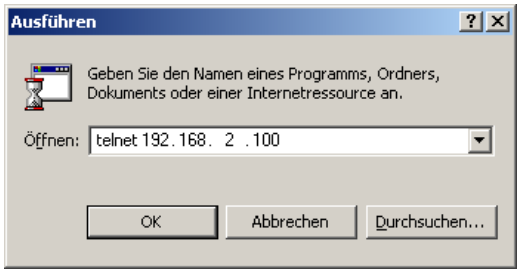


Bild 4-59 Aufruf/Aufbau der Telnet-Verbindung

4.5.2 Funktionen des Telnet-Interfaces

Im Telnet-Interface stehen Ihnen folgende Funktionen zur Verfügung:

- Einstellung der IP-Parameter
- Auswahl des Adressierungsmechanismus
- Rücksetzen auf Werkseinstellungen
- Aktivierung/Deaktivierung des Webservers, der Telnet-Funktion und SNMP
- Aktivierung/Deaktivierung von Port-Security, Access Control for Web
- Umschalten des VLAN-Modes
- Umschalten des Operating-Modes
- Aktivierung/Deaktivierung des Redundanz-Mechanismus RSTP
- Reset

Vorgenommene Einstellungen werden mit „APPLY“ nur übernommen, aber **nicht** dauerhaft gespeichert. Eine dauerhafte Speicherung der jetzigen Konfigurationseinstellungen erreichen Sie mit „SAVE“.

Aufbau der Seiten des Telnet-Interfaces

Login Screen

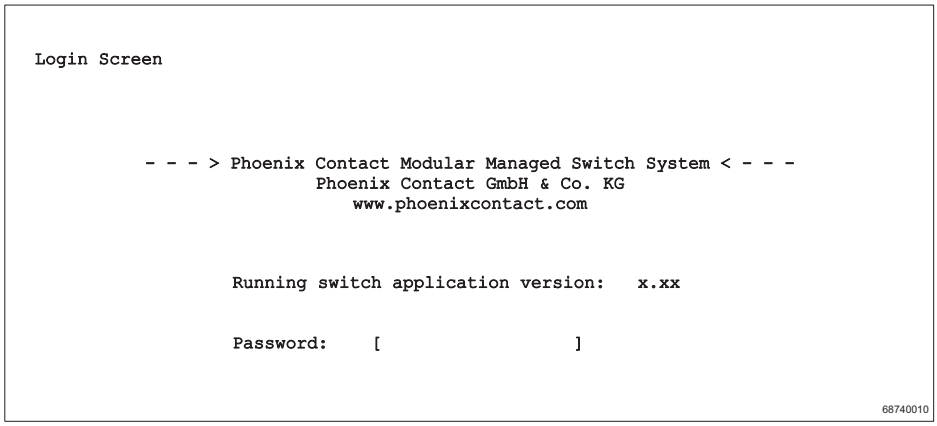


Bild 4-60 Startseite des User-Interfaces

Auf der Startseite erfahren Sie die Version der verwendeten Firmware. Für weitere Einstellungen ist die Eingabe des Passwortes erforderlich. Im Auslieferungszustand lautet das Passwort „private“. Beachten Sie dabei die Groß-/Kleinschreibung. Es wird dringend empfohlen das Passwort zu ändern.

Basic Switch Configuration

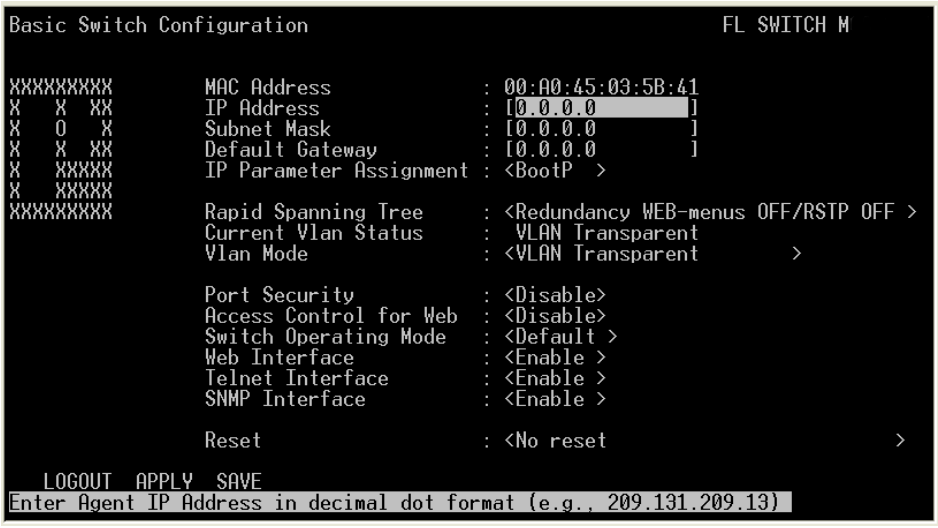


Bild 4-61 IP-Konfiguration im User-Interface

Neben der Anzeige der fest eingestellten MAC-Adresse haben Sie hier die Möglichkeit, die IP-Parameter auszulesen oder zu verändern.

Um die IP-Parameter einstellen zu können, muss bei „IP Parameter Assignment“ die Option „Static“ gewählt sein.

Vorgenommene Einstellungen werden mit „APPLY“ nur übernommen, aber **nicht** dauerhaft gespeichert. Eine dauerhafte Speicherung der jetzigen Konfigurationseinstellungen erreichen Sie mit „SAVE“.

Rücksetzen auf Werkseinstellungen

Wählen Sie auf der Seite „Basic Switch Configuration“ den Punkt „Reset“. Hier können Sie jetzt die Art des Resets auswählen.

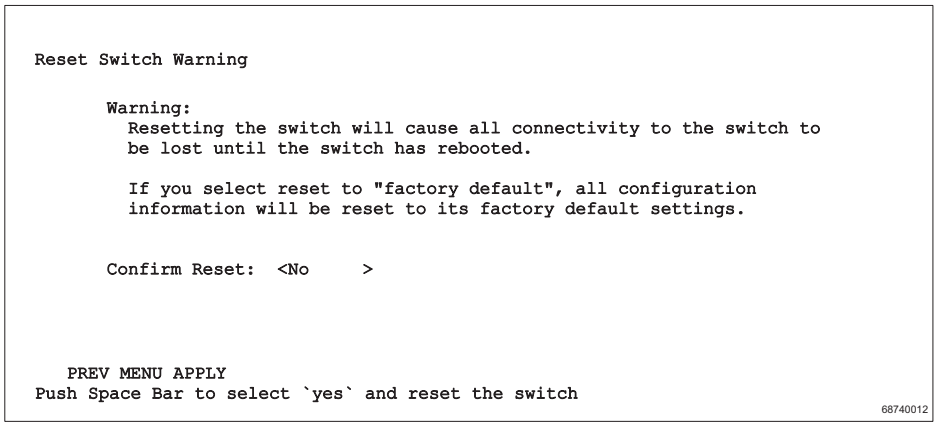

Reset Switch Warning
Warning:
Resetting the switch will cause all connectivity to the switch to be lost until the switch has rebooted.
If you select reset to "factory default", all configuration information will be reset to its factory default settings.
Confirm Reset: <No >
PREV MENU APPLY
Push Space Bar to select `yes` and reset the switch
68740012

Bild 4-62 Rücksetzen auf Werkseinstellungen

Auf dieser Seite haben Sie die Möglichkeit, den Switch wieder auf Werkseinstellungen zurückzusetzen. Jede Konfigurationsänderung wird rückgängig gemacht, alle IP-Parameter werden in den Auslieferungszustand (siehe Kapitel 3.1.1 auf Seite 3-1) zurückgesetzt.

Das Rücksetzen auf Werkseinstellungen setzt auch das Passwort auf „private“ zurück. Aus Sicherheitsgründen wird die Änderung auf ein neues, nur Ihnen bekanntes Passwort empfohlen.

5 (Rapid) Spanning Tree

5.1 Allgemeine Funktion

Beachten Sie beim Betrieb von MRP (Medien-Redundanz-Protokoll), dass (R)STP auf den Ports abgeschaltet wird, die als MRP-Ringports konfiguriert sind.

Loops

Das Rapid/Spanning-Tree-Protokoll (RSTP) ist ein standardisiertes Verfahren (IEEE 802.1w / IEEE 802.1d), das Ethernet-Netzwerke mit redundanten Datenpfaden erlaubt. Ethernet-Netzwerke mit redundanten Datenpfaden bilden eine vermaschte Topologie mit zunächst unzulässigen Schleifen (Loops). Diese Loops führen dazu, dass Datenpakete endlos im Netzwerk kreisen oder auch dupliziert werden können. Die Folge ist in der Regel eine Überlastung des Netzwerkes durch kreisende Datenpakete und damit eine Unterbrechung der Kommunikation. Daher wird die vermaschte Struktur, mit Hilfe des Spanning-Tree-Algorithmus, durch einen logischen, deterministischen Pfad in Form einer Baumstruktur ersetzt, in dem sich keine Loops mehr befinden. Bei Ausfall von Datenpfaden werden die vorher abgeschalteten Verbindungen teilweise wieder zugeschaltet, so dass ein unterbrechungsfreier Betrieb des Netzwerkes gewährleistet ist.

IEEE 802.1w

Das Rapid Reconfiguration Spanning-Tree-Protokoll ist ein standardisiertes Verfahren (IEEE 802.1w), das Ethernet-Netzwerke mit redundanten Datenpfaden erlaubt und die langen Timer-gesteuerten Umschaltzeiten von STP vermeidet. Der formale Begriff „Rapid Reconfiguration Spanning Tree“ wird üblicherweise nicht verwendet, man spricht einfach vom „Rapid Spanning Tree Protocol - (R)STP“.

Beispiel:

In der nachfolgenden Netzwerktopologie sind (sechs) redundante Pfade geschaffen, um bei Ausfall eines Datenpfades weiterhin alle Teilnehmer im Netz erreichen zu können. Diese redundanten Pfade sind unzulässige Loops. Das Spanning-Tree-Protokoll überführt diese Topologie automatisch durch Abschalten ausgewählter Ports in einen Baum. Dabei wird einer der Switches als „Wurzel“ (Root) des Baumes ausgewählt. Von der Root aus ist jeder andere Switch über genau einen Datenpfad erreichbar.

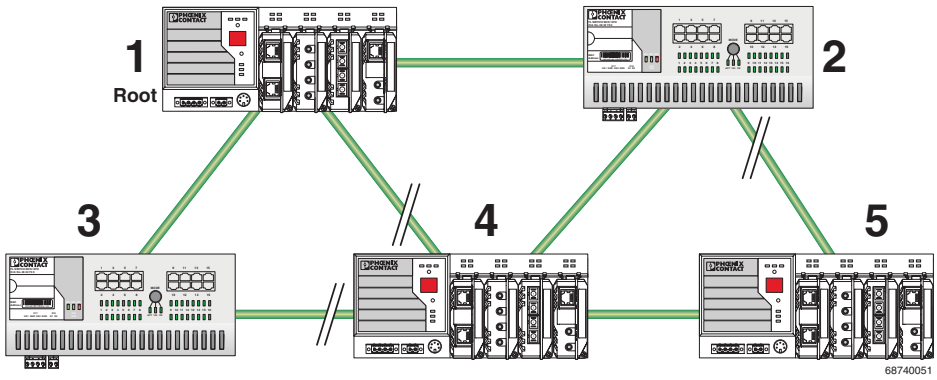


Bild 5-1 Mögliche Baumstruktur mit Spanning Tree

5.2 Inbetriebnahme von (R)STP

Die Inbetriebnahme besteht aus zwei Teilen, die in angegebener Reihenfolge ausgeführt werden müssen:

1 Einschalten von (R)STP auf allen Switches, die als aktive (R)STP-Komponenten im Netzwerk betrieben werden sollen.

2 Verbinden der Switches zu einer vermaschten Topologie.

Stellen Sie die vermaschte Topologie erst her, nachdem Sie (R)STP aktiviert haben.

5.2.1 Einschalten von (R)STP auf allen beteiligten Switches

(R)STP kann über das Web Based Management, über das SNMP-Interface, über die serielle Schnittstelle oder über Telnet aktiviert werden.

Während der Switch die Netzwerktopologie erlernt, nimmt er kurzzeitig nicht an der Netzkommunikation teil.

5.2.1.1 Einschalten mittels Web Based Management

Starten Sie das Web Based Management der Switches, z. B. mit dem Factory Manager. Wechseln Sie im Menü „General Configuration“, dann auf die Seite „User Interfaces“. Aktivieren Sie unter „Redundancy “ die Funktion „(Rapid) Spanning Tree“ und bestätigen Sie mit Ihrem Passwort.

Mit der Aktivierung von „(Rapid) Spanning Tree“ unter „User Interfaces“ ist der Redundanz-Mechanismus **nicht** aktiviert. Es wird im WBM-Menü die Seite „(Rapid) Spanning Tree“, unter dem die Funktion konfiguriert und aktiviert werden kann, freigeschaltet.

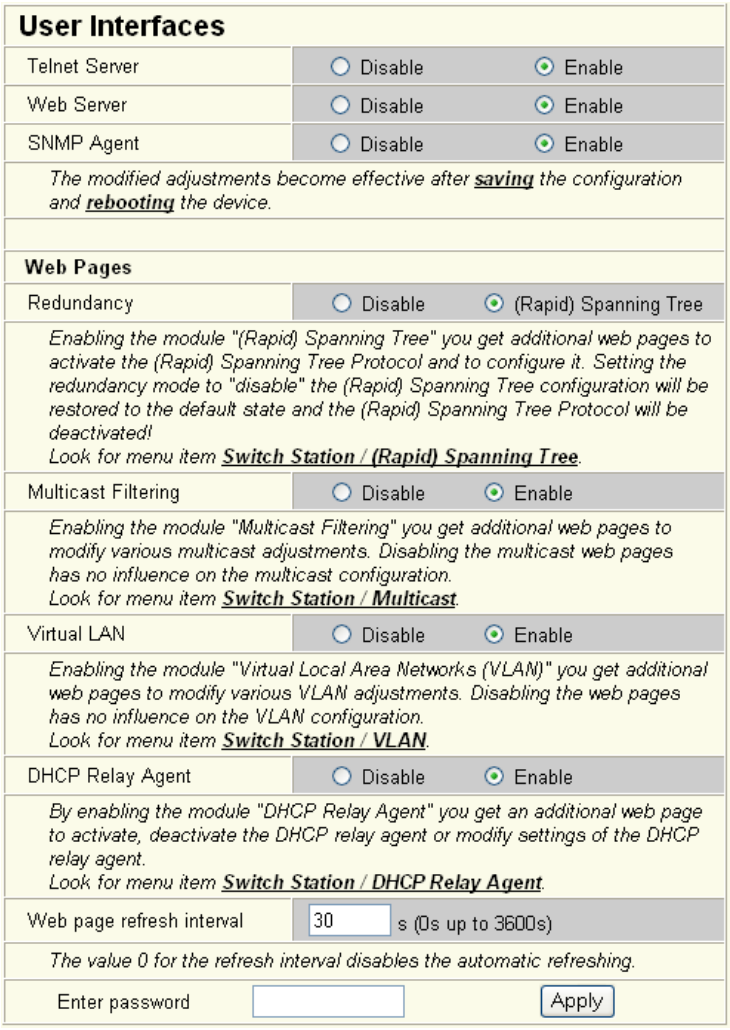
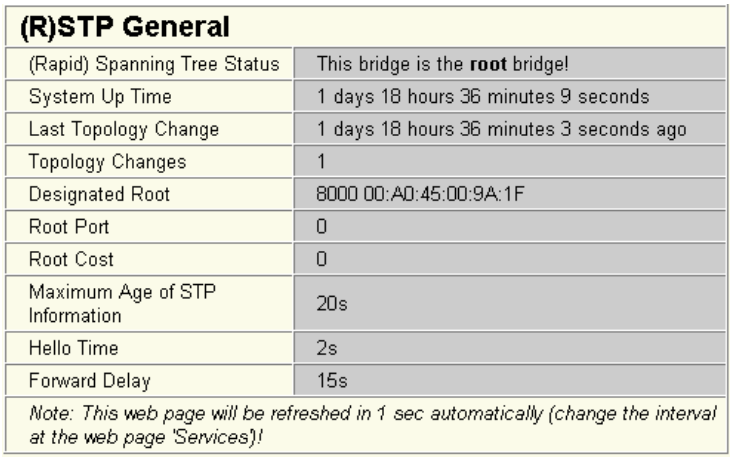

User Interfaces
Telnet Server
Disable
Enable
Web Server
Disable
Enable
SNMP Agent
Disable
Enable
The modified adjustments become effective after saving the configuration and rebooting the device.
Web Pages
Redundancy
Disable
(Rapid) Spanning Tree
Enabling the module "(Rapid) Spanning Tree" you get additional web pages to activate the (Rapid) Spanning Tree Protocol and to configure it. Setting the redundancy mode to "disable" the (Rapid) Spanning Tree configuration will be restored to the default state and the (Rapid) Spanning Tree Protocol will be deactivated!
Look for menu item Switch Station / (Rapid) Spanning Tree.
Multicast Filtering
Disable
Enable
Enabling the module "Multicast Filtering" you get additional web pages to modify various multicast adjustments. Disabling the multicast web pages has no influence on the multicast configuration.
Look for menu item Switch Station / Multicast.
Virtual LAN
Disable
Enable
Enabling the module "Virtual Local Area Networks (VLAN)" you get additional web pages to modify various VLAN adjustments. Disabling the web pages has no influence on the VLAN configuration.
Look for menu item Switch Station / VLAN.
DHCP Relay Agent
Disable
Enable
By enabling the module "DHCP Relay Agent" you get an additional web page to activate, deactivate the DHCP relay agent or modify settings of the DHCP relay agent.
Look for menu item Switch Station / DHCP Relay Agent.
Web page refresh interval
30
s (0s up to 3600s)
The value 0 for the refresh interval disables the automatic refreshing.
Enter password
Apply

Bild 5-2 Menü „User Interfaces“

Wird nach Konfiguration von (R)STP der Punkt „Redundancy“ auf der Web-Seite „User Interfaces“ auf „Disable“ gesetzt, geht die zuvor erstellte Konfiguration verloren und die Web-Seiten für (R)STP werden ausgeblendet.

Wechseln Sie jetzt in das Menü „Switch Station“ auf der Seite „(R)STP General“. Hier finden Sie verschiedene Informationen zur Spanning-Tree-Konfiguration.



(R)STP General

(Rapid) Spanning Tree Status	This bridge is the **root** bridge!
System Up Time	1 days 18 hours 36 minutes 9 seconds
Last Topology Change	1 days 18 hours 36 minutes 3 seconds ago
Topology Changes	1
Designated Root	8000 00:A0:45:00:9A:1F
Root Port	0
Root Cost	0
Maximum Age of STP Information	20s
Hello Time	2s
Forward Delay	15s

Note: This web page will be refreshed in 1 sec automatically (change the interval at the web page 'Services')!

Bild 5-3 (R)STP General

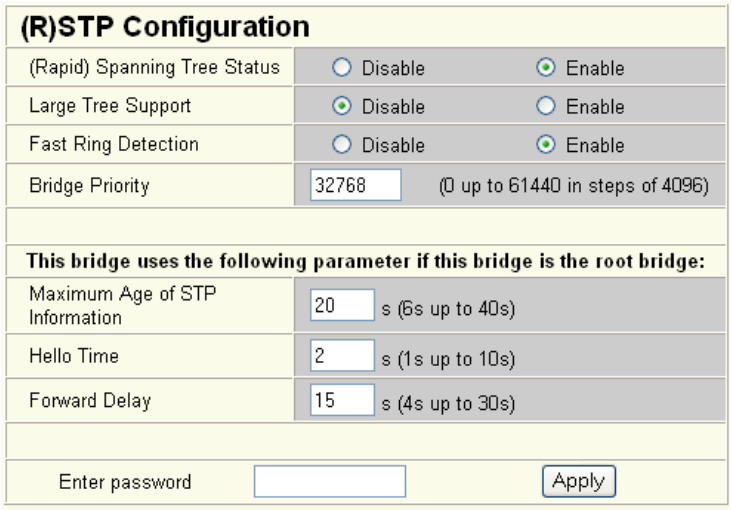
Die Webseite zeigt die Parameter, mit denen der Switch aktuell arbeitet.

(R)STP Configuration

Um (R)STP mit Default-Einstellung zu starten, genügt es, den Rapid-Spanning-Tree-Status auf „Enable“ zu setzen. Es können für den Switch Prioritätswerte festgelegt werden. Über diese Prioritätswerte können Bridge und Backup-Root bestimmt werden.

Zulässig sind nur Vielfache von 4096. In das Feld „Priority“ können Sie den gewünschten Wert eintragen. Der Wert wird automatisch auf das nächstgelegene Vielfache von 4096 gerundet. Nachdem Sie mit Ihrem Passwort die Änderung bestätigt haben, wird der Initialisierungs-Mechanismus gestartet.

Jetzt können Sie die redundanten Verbindungen herstellen.



(R)STP Configuration

(Rapid) Spanning Tree Status	○ Disable	◉ Enable
Large Tree Support	◉ Disable	○ Enable
Fast Ring Detection	○ Disable	◉ Enable
Bridge Priority	32768	(0 up to 61440 in steps of 4096)
This bridge uses the following parameter if this bridge is the root bridge:		
Maximum Age of STP Information	20	s (6s up to 40s)
Hello Time	2	s (1s up to 10s)
Forward Delay	15	s (4s up to 30s)
Enter password		Apply

Bild 5-4 (R)STP Configuration

Large Tree Support
Wird RSTP mit Default-Werten betrieben, ist es für bis zu sieben Switches entlang des relevanten Pfades (siehe Bild 5-19 auf Seite 5-25 und Bild 5-20 auf Seite 5-26 als Beispiel für den relevanten Pfad) geeignet. Damit wäre das RSTP-Protokoll in einer Ringtopologie für bis zu 15 Switches möglich.

Durch die Option „Large Tree Support“ ist die Ringtopologie unter Verwendung von RSTP für 28 Switches entlang des relevanten Pfades geeignet. Durch die Large-Tree-Support-Option wäre eine RSTP-Ringtopologie mit bis zu 57 Geräten möglich. Bei der Verwendung von Large-Tree-Support ist folgendes zu beachten:

– Verwenden Sie in der Large-Tree-Support-RSTP-Topologie **keine** Geräte, die den Large Tree Support **nicht** unterstüzen.
– Schalten Sie die Large-Tree-Support-Option auf **allen** Geräten ein.
– Wenn in einem bestehenden Netzwerk mit mehr als sieben Switches entlang des relevanten Pfades RSTP als Redundanz-Mechanismus aktiviert werden soll, muss zuvor die Large-Tree-Support-Option auf allen Geräten eingeschaltet werden.
– Es wird empfohlen, Large-Tree-Support in Netzen mit weniger als sieben Switches entlang des relevanten Pfades nicht zu aktivieren.

Maximum Age of STP information
Der Parameter wird vom Root-Switch gesetzt und von allen Switches im Ring benutzt. Der Parameter wird versendet, um sicherzustellen, dass jeder Switch im Netzwerk einen konstanten Wert hat, gegen den das Alter der gespeicherten Konfiguration getestet wird.

Die Felder „Maximum Age of STP Information“, „Hello Time“ und „Forward Delay“ haben dieselbe Bedeutung wie beim STP. Diese Werte werden genutzt, wenn dieser Switch zur Root wird. Die zur Zeit tatsächlich genutzten Werte finden Sie unter (R)STP-General.

Hello Time
Gibt das Zeit-Intervall an, innerhalb dessen sich die Root-Bridge regelmäßig über BPDU bei den anderen Brücken meldet.

Forward Delay
Der Forward-Delay-Wert zeigt an, wie lange die Switches warten sollen, um den Zustand eines Ports im STP-Modus von „discarding“ zu „listening“ und von „listening“ nach „learning“ zu wechseln (2 x Forward Delay).

Die Parameter „Max Age of STP“, „Hello Time“ und „Forward Delay“ sind im Auslieferungszustand optimiert. Sie sollten nicht verändert werden.

(R)STP Port Table

(R)STP Port Table

Module	Interface	Port	Oper Edge Port	Protocol	STP State
HS	X1	1	edge port	RSTP	forwarding
		2	edge port	RSTP	discarding
	X2	3	edge port	RSTP	discarding
		4	edge port	RSTP	discarding
	X3	5	edge port	RSTP	discarding
		6	edge port	RSTP	discarding
	X4	7	edge port	RSTP	forwarding
		8	edge port	RSTP	discarding

Note: This web page will be refreshed in 22 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces')!

Bild 5-5 (R)STP Port Table

Oper Edge Port
Alle Ports, an denen keine (R)STP-BPDUs empfangen werden (z. B. Endgeräte-Ports), werden zum Edge-Port, also Ports, die nach Neustart sofort in den Zustand „Forwarding“ gehen.

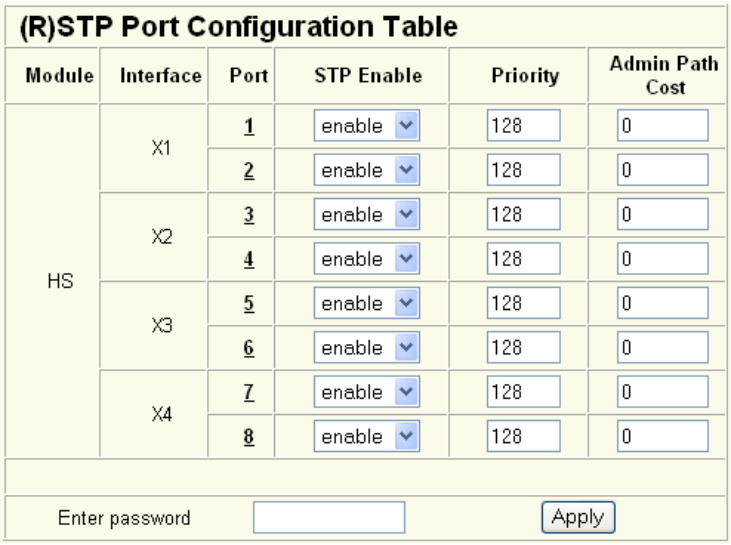
Protocol
Zeigt das verwendete Redundanz-Protokoll.

(R)STP State
Zeigt den aktuellen (R)STP-Zustand des jeweiligen Ports an.

Mögliche Zustände sind:

– „Forwarding“
  Der Port ist in die aktive Topologie eingebunden und leitet Daten weiter.
– „Discarding“
  Der Port nimmt nicht an der Datenübertragung teil.
– „Learning“
  Der Port nimmt nicht an der Datenübertragung der aktiven Topologie teil, aber MAC-Adressen werden erlernt.
– Blocking/Discarding
  Der Port besitzt einen Link, ist aber vom RSTP in den Zustand „Discarding“ versetzt worden.

(R)STP Port Configuration Table



(R)STP Port Configuration Table

Module	Interface	Port	STP Enable	Priority	Admin Path Cost
HS	X1	1	enable	128	0
		2	enable	128	0
	X2	3	enable	128	0
		4	enable	128	0
	X3	5	enable	128	0
		6	enable	128	0
	X4	7	enable	128	0
		8	enable	128	0

Enter password Apply

Bild 5-6 Menü „(R)STP Port Configuration Table“

Hier finden Sie einen Überblick über die wesentlichen Einstellungen pro Port.

5.2.1.2 (R)STP Port Configuration

Änderungen der Eigenschaften können eine komplette Neukonfiguration des (Rapid) Spanning Tree zur Folge haben.

Es wird empfohlen, einen geeigneten Root-Switch und einen Backup-Root-Switch durch entsprechende Prioritätsvergabe zu bestimmen.

Auf dieser Seite sind die gültigen (R)STP-Konfigurationseinstellungen für den jeweils ausgewählten Port dargestellt.

Wenn über einen Port Endgeräte oder Subnetze ohne RSTP oder STP verbunden sind, empfiehlt es sich, den „Admin Edge Port“ auf „Edge Port“ zu setzen. Dadurch wird durch eine Link-Änderung an diesem Port keine Topologie-Änderung veranlasst.

5.2.1.3 Switch/Port-ID

Die Wertigkeit der Switches und der Ports wird nach sogenannten Prioritätsvektoren ermittelt.

Bridge-Identifier

Eine Switch-ID besteht aus acht Byte als vorzeichenfreier Integer-Wert. Beim Vergleich zweier Switch-IDs ist diejenige die höhere „bessere“ Priorität, deren numerischer Wert niedriger ist.

Die zwei vorderen Bytes beinhalten die Priorität.
Die letzten sechs Byte enthalten die MAC-Adresse und stellen damit die Eindeutigkeit der Switch-ID bei gleicher Priorität sicher.

Der Switch mit der niedrigsten numerischen Switch-ID wird die Root. Es wird empfohlen, über die Priorität Root- und Alternate-Port festzulegen.

Port-Identifier

Die Port-ID besteht aus vier Bits für die Portpriorität und zwölf Bits für die Portnummer. Die Port-ID wird als vorzeichenfreier Integer-Wert interpretiert. Beim Vergleich zweier Port-IDs ist diejenige die höhere „bessere“ Priorität, deren numerischer Wert niedriger ist.

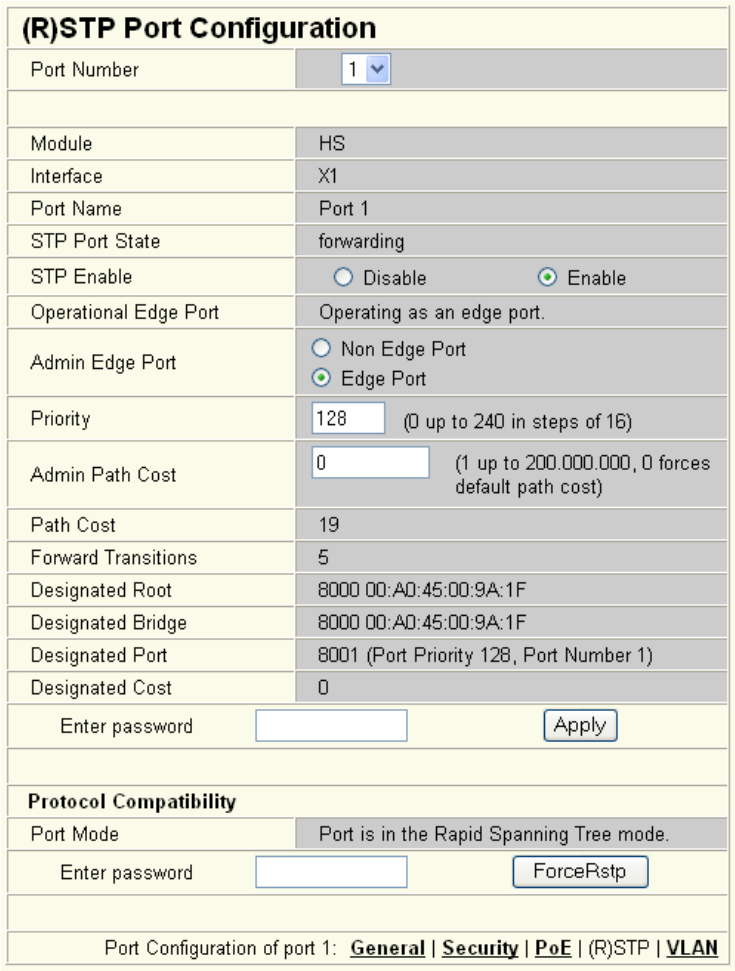


Bild 5-7 (R)STP Port Configuration

Port Number
Zeigt die Nummer des aktuell ausgewählten Ports.

Port Name
Zeigt den Namen des Ports.

STP Port State
Zeigt, mit welchen Status dieser Port im STP teilnimmt.

Operational Edge Port
Zeigt, ob dieser Port als Edge-Port betrieben wird.

Admin Edge Port
Hier können Sie einstellen, dass dieser Port, wenn möglich, als Edge-Port (Default-Einstellung) betrieben werden soll.

Priority
Zeigt die für diesen Port eingestellte Priorität an (Default 128). Aufgrund der Abwärtskompatibilität zu STP sind Prioritätswerte einstellbar, die beim RSTP nicht konfigurierbar sind.

Admin Path Cost
Zeigt die für diesen Port eingestellten Pfad-Kosten an. Path Cost gleich „0“ aktiviert die Berechnung der Kosten in Abhängigkeit der Übertragungsgeschwindigkeit (10 MBit/s = 100; 100 MBit/s = 19).

Path Cost
Zeigt die für diesen Port verwendeten Pfad-Kosten an.

Forward Transitions
Nennt die Anzahl, wie oft der Port vom Zustand „Discarding“ in den Zustand „Forwarding“ gewechselt ist.

Die weiteren Parameter geben Auskunft über die von den BPDU-Telegrammen benutzten Netzwerkpfade in einer stabilen Topologie.

Designated Root
Root-Bridge für diesen Spanning Tree.

Designated Bridge
Der Switch, von dem der Port die besten BPDUs erhält. Der Wert setzt sich aus dem Prioritätswert in Hex und der MAC-Adresse zusammen.

Designated Port
Port, über den die BPDUs von der Designated Bridge gesendet werden. Der Wert setzt sich aus der Port-Priorität (2-stellig) und der Port-Nummer zusammen.

Designated Cost
Zeigt die Pfadkosten dieses Segments zum Root-Switch.

Protocol Compatibility

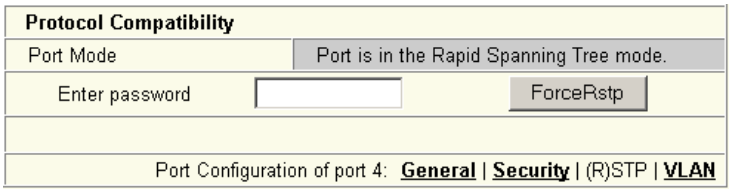

Protocol Compatibility
Port Mode
Port is in the Rapid Spanning Tree mode.
Enter password
ForceRstp
Port Configuration of port 4: General | Security | (R)STP | VLAN

Bild 5-8 Protocol Compatibility

Empfängt ein Port STP-BPDUs, so wechselt er selbstständig in den STP-Modus. Ein automatischer Wechsel in den (R)STP-Modus findet nicht statt, ein Wechsel in den (R)STP-Modus kann nur durch den Button „Force (R)STP“ oder durch einen Neustart erzwungen werden.

RSTP Fast Ring Detection

Sie können die Funktion „RSTP Fast Ring Detection“ auf der Web-Seite „RSTP Configuration“ aktivieren (siehe Seite 5-4).

Diese Funktion beschleunigt die Umschaltung auf einen redundanten Pfad im Fehlerfall und ermöglicht eine einfache Diagnose. Durch die RSTP Fast Ring Detection wird jedem Ring eine ID gegeben, diese ID wird jedem Switch in dem jeweiligen Ring bekannt gemacht. Ein Switch kann gleichzeitig mehreren unterschiedlichen Ringen angehören.

Aufbau der Ring-ID

Die Ring-ID bildet sich aus der Port-Nummer des blokierenden Ports und der MAC-Adresse des zugehörigen Switches. Vorteile durch die Ring-ID:

– Redundante Wege können leichter identifiziert und blockierende Ports leichter gefunden werden.
– Die Kontrolle, ob die Wunschtopologie der tatsächlichen Topologie entspricht, wird ermöglicht.

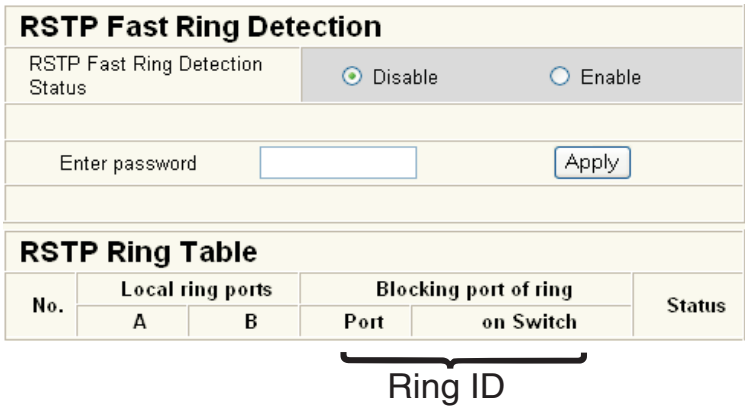


Bild 5-9 RSTP Ring Table

Informationen im WBM

Auf der Webseite (und über SNMP) werden folgende Informationen angezeigt:

Lokal ring ports
Diese beiden Ports dieses Switches gehören dem aufgeführten Ring (Ring ID) an.

Blockierender Port
Dieser Port unterbricht gewollt den Loop.

Ring Detection Stati

Folgende Stati können bei der Ringerkennung auftreten:

– **Not Ready** - Die Ringerkennung ist noch nicht abgeschlossen.
– **OK** - Die Ringerkennung ist abgeschlossen und die schnelle Umschaltung im Fehlerfall ist möglich.
– **Breaked** - Der Ring ist an diesem Ast in Richtung des Root-Switches unterbrochen.
– Failed on Port A - Der Ring wurde auf diesem Switch an Port A unterbrochen.

Bei einem Link-Ausfall im Ring wird der Trap „trapRstpRingFailure“ gesendet.

Falls der Status „Breaked“ oder „Failed“ für länger als 60 Sekunden besteht, wird er nach der nächsten Topologieänderung nicht mehr angezeigt, da diese Ringe nicht länger existent sind.

Bei der Verwendung der RSTP Fast Ring Detection ist folgendes zu beachten:

– Verwenden Sie bei der RSTP Fast Ring Detection **keine** Geräte, die diese Funktion **nicht** unterstützen.
– Schalten Sie die RSTP Fast Ring Detection auf **allen** Geräten ein.
– Alle Datenpfade müssen im Voll-Duplex-Betrieb sein.

5.2.1.4 Umschaltzeiten von Fast Ring Detection

Bei der maximal zulässigen Anzahl von 57 Switches im Ring lässt sich die Umschaltzeit der nachfolgenden Grafik entnehmen.

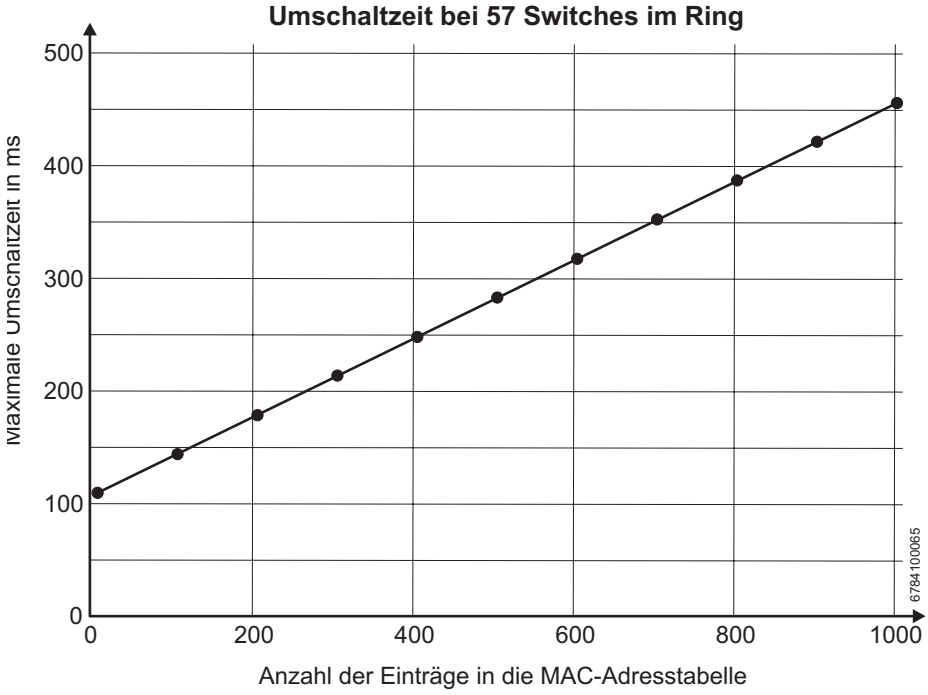


Bild 5-10 Umschaltzeiten bei maximalem Ring mit 57 Switches

5.2.2 Verbindungsausfall - Beispiel

In der nachfolgenden Grafik ist ein RSTP-Ring mit sechs Switches dargestellt, in dem Switch 1 die Root ist. Der Ring erstreckt sich jeweils über Port 1 und Port 2 bei jedem Switch. Am Switch 4 wird durch einen blockierenden Port die Schleife unterbrochen.

Kommt es jetzt zu einer Leitungsunterbrechung an der mit dem Stern markierten Stelle, führt das zu folgenden Einträgen auf der Webseite „RSTP Fast Ring Detection“:

Switch 3 - Failed on Port A

Switch 4 - Broken

Zuätzlich würde Switch 3 den Trap „flWorkLinkFailure“ generieren, sofern das Versenden von Traps nicht abgeschaltet ist.

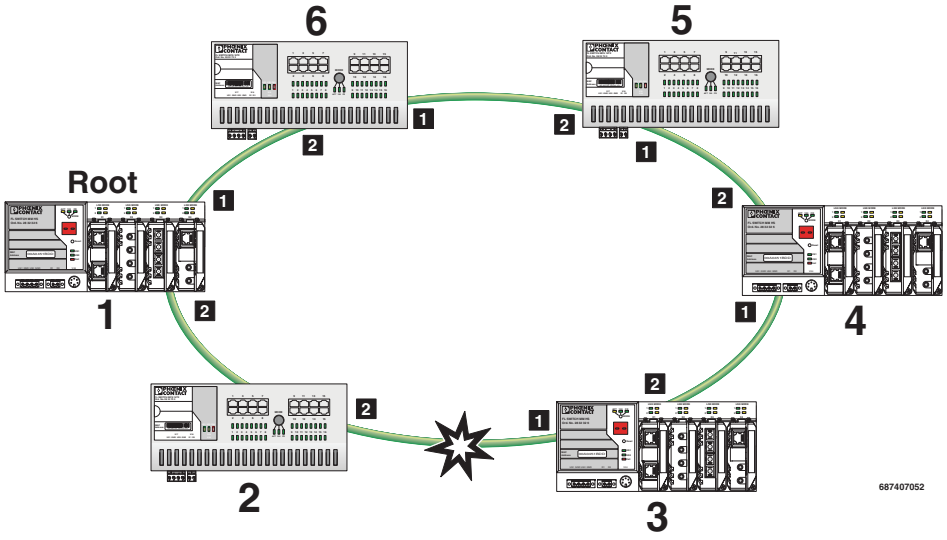


Bild 5-11 Verbindungsausfall mit RSTP Ring Detection

5.2.3 Mischbetrieb zwischen RSTP und STP

Falls ein Teilnehmer mit STP-Unterstützung ins Netzwerk integriert wird, werden nur die Ports des Switches in den STP-Modus geschaltet, an denen STP-BPDUs empfangen werden. Alle anderen Ports, an denen RSTP-BPDUs empfangen werden, bleiben im RSTP-Modus.

5.2.4 Topologie-Erkennung eines Rapid-Spanning-Tree-Netzwerkes (RSTP)

(Rapid)Spanning-Tree-Switches tauschen untereinander ständig Informationen über die Netzwerktopologie mittels spezieller Nachrichten (BPDUs - Bridge Protocol Data Units) aus. Somit „lernen“ die Switches die aktuelle Netzwerktopologie kennen und treffen basierend auf diesen Informationen folgende Entscheidungen:

– Welcher Switch wird als Root-Switch ausgewählt und
– welche Datenpfade werden abgeschaltet.

Wenn ein Switch unter Verwendung des (Rapid) Spanning-Tree-Protokolls gestartet wird, nimmt er zunächst an, dass er selbst der Root-Switch ist. Gleichzeitig ist in der Startphase keine Datenkommunikation möglich, bis die aktuelle Netzwerktopologie erlernt wurde und die oben angegebenen Entscheidungen getroffen sind. Somit werden Loops, die in der Startphase des Netzwerkes dadurch entstehen können, dass kein Datenpfad unterbrochen ist, vermieden.

5.2.4.1 Topologie-Änderung

Eine Topologie-Änderung kann ausgelöst werden durch:

– Hinzukommen eines Datenpfades,
– Ausfall eines Datenpfades,
– Hinzukommen eines Spanning-Tree-Switches oder
– Ausfall eines Spanning-Tree-Switches.

Eine Topologie-Änderung wird automatisch erkannt und das Netz wird so rekonfiguriert, dass wieder ein Baum entsteht und alle Geräte in dem Baum erreichbar sind. Dabei treten auch vorübergehend keine Schleifen auf.

Falls das Versenden von Traps nicht deaktiviert wurde, werden zwei Traps generiert:

– newRoot (OID: 1.3.6.1.2.1.17.0.1) und
– topologyChange (OID 1.3.6.1.2.1.17.0.2).

5.2.4.2 Unterbrochene Datenpfade und Port-Zustände

Die beschriebene Unterbrechung von Datenpfaden durch das Spanning-Tree-Protokoll wird hergestellt, indem einzelne Ports abgeschaltet werden und keine Datenpakete weiterleiten. Ein Port kann folgende Zustände annehmen:

– Learning
– Forwarding
– Blocking/Discarding
– Disabled (Link Down oder vom Benutzer abgeschaltet)

Die aktuellen Port-Stati werden im Web-Interface angezeigt.

Die Eigenschaften der unterschiedlichen Port-Stati finden Sie in der nachfolgenden Tabelle.

Tabelle 5-1 Eigenschaften der Port-Stati

	Empfang und Auswertung von BPDUs (Topologie erlernen)	MAC-Adressen der angeschlossenen Geräte lernen und Switching-Tabelle aufbauen	Datenpakete weiterleiten (normale Switching-Funktionalität)
Disabled			
Blocking/Discarding	X		
Learning	X	X	
Forwarding	X	X	X

Die Abfolge der fünf im Spanning Tree Protocol definierten Port-Zustände ist nicht frei. In der folgenden Grafik ist die Mögliche Abfolge der Port-Zustände dargestellt.

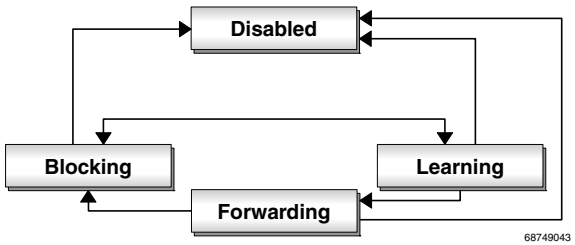


Bild 5-12 Abfolge der möglichen Port-Zustände im STP

Ein Port durchläuft nach dem Gerätestart und ggfs. auch bei einer Änderung der Topologie die Zustände in folgender Reihenfolge:

Learning → Forwarding

oder

Disabled → Blocking/Discarding

Aufgrund der Edge-Eigenschaft der Ports schalten diese sofort in „Forwarding“ um. Im zweiten Fall erzeugt der Port eine Unterbrechung eines Datenpfades, um Loops entsprechend zu unterdrücken.

An einem Datenpfad zwischen zwei Spanning-Tree-Switches ist immer mindestens ein Port im Status „Forwarding“, um den Datenpfad in das Netzwerk einzubinden.

5.2.4.3 Fast Forwarding

Wird an einem Port das Spanning-Tree-Protokoll deaktiviert, so befindet sich der entsprechende Port im sog. „Fast Forwarding“-Betrieb.

Ein Fast-Forwarding-Port

– ignoriert alle BPDUs, die an diesem Port empfangen werden,
– sendet keine BPDUs und
– wechselt sofort nach Herstellung der Datenverbindung (Link) in den Status „Forwarding“. An diesem Port angeschlossene Endgeräte sind sofort erreichbar.

Zum Aktivieren von Fast Forwarding muss im WBM auf der Seite „STP Port Configuration“ der Punkt „Port STP Status“ auf „Disabled“ gesetzt werden.

Frame-Duplizierung

Durch die schnellen Umschaltzeiten von RSTP kann es zu einer Frame-Duplizierung und zur Änderung der Frame-Reihenfolge kommen.

5.2.4.4 Einschalten über serielle Schnittstelle oder Telnet

Stellen Sie eine Verbindung zum Switch her. Das Vorgehen ist im Kapitel „Management über lokale V.24-Kommunikationsschnittstelle“ auf Seite 4-121 oder im Kapitel „Management über Telnet“ auf Seite 4-128 beschrieben. Stellen Sie auf der nachfolgenden Seite im Feld „Redundancy“ den Wert „Spanning Tree, Enabled“ ein und wählen Sie „Save“.

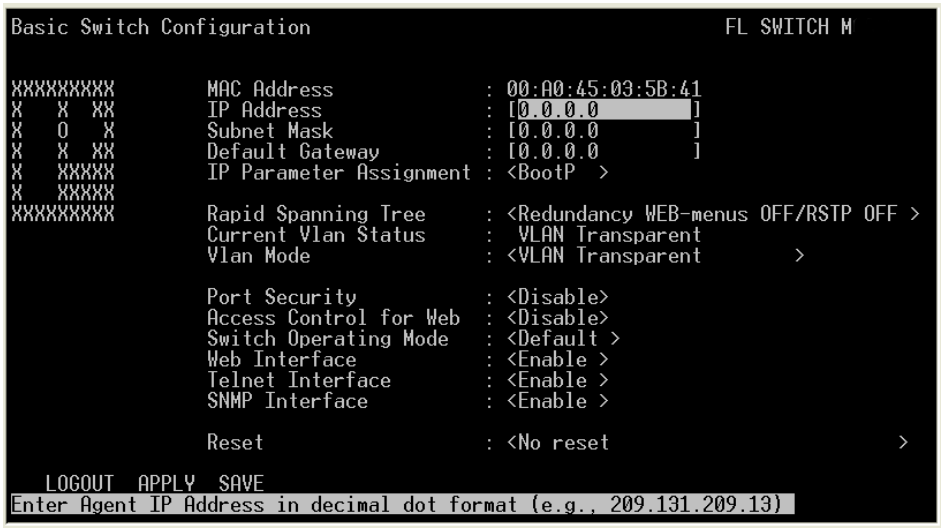


Bild 5-13 Aktivierung von Rapid Spanning Tree

5.2.5 Projektierungshinweise zu Rapid Spanning Tree

Das Rapid-Spanning-Tree-Verfahren zeichnet sich gegenüber dem Spanning-Tree-Verfahren dadurch aus, dass Aktionen ereignisgesteuert und nicht mehr timerbasiert ausgelöst werden.

Fällt eine Leitung aus (Link Down) kann das Rapid-Spanning-Tree-Verfahren schneller auf den Ausfall reagieren und so die Umschaltzeit gering halten.

Damit die RSTP-Switches einen Leitungsausfall sowie eine Leitungswiederherstellung schnell erkennen können, muss am Switch ein Link Down oder Link Up erkannt werden. Bitte betrachten Sie hier insbesondere Strecken, bei denen Medienkonverter eingesetzt werden. Ggfs. bieten Medienkonverter Einstellmöglichkeiten, um den Link-Status der LWL-Seite auf die Twisted-Pair-Seite zu übertragen.

Wenn ein Link Down am Switch nicht erkannt wird, weil die Leitungsunterbrechung zwischen Medienkonvertern auftritt und diese keinen Link Down am Switch erzwingen, kommt die Timer-basierte Erkennung zum Tragen, die zu längeren Umschaltzeiten führen kann.

- Für kurze Umschaltzeiten sollten Sie Ihr Netzwerk so strukturieren, dass max. sieben Switches in einer Kaskade bis zum Root-Switch liegen. Die Umschaltzeiten können in der Größenordnung 100 ms bis 2 s liegen.
- Legen Sie über die Vergabe der Priorität einen zentralen Switch als Root fest.
- Es empfiehlt sich ebenfalls, einen Switch als Back-Up-Root zu bestimmen.
- Für kurze Umschaltzeiten sollten alle Switches in der redundanten Topologie das Rapid-Spanning-Tree-Protokoll unterstützen und keine Hubs verwendet werden.

5.2.5.1 Verbinden der Switches zu einer vermaschten Topologie

Nachdem Sie (Rapid) Spanning Tree bei allen Switches eingeschaltet haben, können Sie eine vermaschte Topologie mit redundanten Datenpfaden aufbauen. Sie können jetzt beliebige Datenverbindungen herstellen, ohne dabei auf die Entstehung von Loops zu achten oder auch Sie können absichtlich Loops hinzufügen, um redundante Verbindungen herzustellen.

Ein Datenpfad zwischen Spanning-Tree-Switches kann dabei sein:

- Eine direkte Verbindung.
- Eine Verbindung über einen oder mehrere weitere Switches, die kein Spanning Tree unterstützen.

Falls nicht alle eingesetzten Switches Spanning Tree unterstützen, verlängert sich die Rekonfigurationszeit des Spanning Trees um die Aging Time der Switches ohne Spanning-Tree-Unterstützung.

- Eine Verbindung über einen oder mehrere weitere Hubs, die kein Spanning Tree unterstützen.

Darüber hinaus kann ein Datenpfad auch bestehen aus einer Verbindung eines Spanning-Tree-Switches zu:

- Einem Endgerät.
- Einem aus mehreren Infrastrukturkomponenten (Hubs oder Switches) ohne Spanning-Tree-Unterstützung bestehenden Netzwerksegment, in dem **keine** Loops auftreten dürfen.

Für die letzen beiden Fälle von Datenpfaden sind keine besonderen Vorkehrungen zu treffen. Sie können ggfs. die Option „Fast Forwarding“ für die entsprechenden Ports nutzen (siehe Kapitel „Fast Forwarding“ auf Seite 5-14).
Für die ersten drei genannten Fällen sind folgende Regeln zu beachten:

– **Regel 1: Spanning-Tree-Transparenz aller Infrastrukturkomponenten**
  Alle eingesetzten Infrastrukturkomponenten in Ihrem Netzwerk, die Spanning Tree nicht aktiv unterstützen, müssen transparent für Spanning-Tree-Nachrichten (BPDUs) sein und alle BPDUs unverändert an alle Ports weiterleiten. Der Switch ist bei abgeschaltetem Spanning Tree transparent für BPDUs.

– **Regel 2: Mindestens eine aktive Spanning-Tree-Komponente pro Loop**
  Eine aktive Spanning-Tree-Komponente unterstützt das Spanning-Tree-Protokoll, sendet/empfängt BPDUs, wertet sie aus und setzt seine Ports in die entsprechenden STP-Zustände.
  In jedem Loop eines Netzwerks muss mindestens eine aktive Spanning-Tree-Komponente vorhanden sein, um den Loop aufzulösen.
  Beispiel:

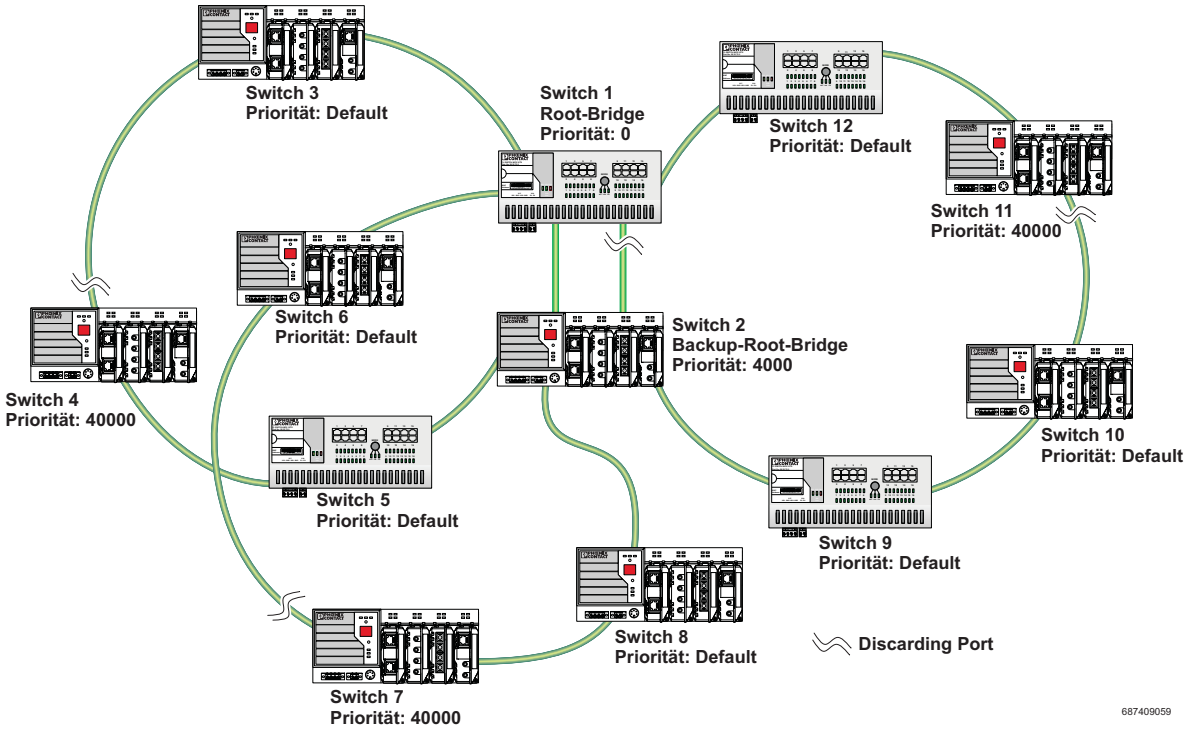


Bild 5-14 Beispieltopologie

Die Loops in der gezeigten Beispieltopologie werden jeweils durch aktive RSTP-Komponenten aufgehoben. In der Beispieltopologie befinden sich drei Ringe, die Root und die Backup-Root sind Komponenten in jedem der drei Ringe. Die drei Ringe beeinflussen sich untereinander nicht, eine Änderung der Topologie in einem Ring beeinflusst nicht die Ttopologie der beiden anderen Ringe

– **Regel 3: Nicht mehr als zehn aktive Spanning-Tree-Komponenten in der Topologie bei Nutzung der Spanning-Tree-Default-Einstellung**
  Die Fähigkeit, beliebige Topologien zu einem Baum ohne Loops auflösen zu können, bedingt ein komplexes Protokoll, das mit mehreren variablen Timern arbeitet. Diese

sind mit den in der IEEE-Norm empfohlenen Default-Werten so dimensioniert, dass eine Topologie mit höchstens zehn aktiven Spanning-Tree-Komponenten in jedem Fall zu einem stabilen Netzwerk führt. Bei der Verwendung von Large-Tree ist Folgendes zu beachten (siehe auch Kapitel „Large Tree Support“ auf Seite 5-5):

– Verwenden Sie in der Large-Tree-Support-RSTP-Topologie **keine** Geräte, die Large Tree **nicht** unterstützen.
– Schalten Sie die Large-Tree-Support-Option auf **allen** Geräten ein.
– Wenn in einem bestehenden Netzwerk mit mehr als sieben Switches entlang des relevanten Pfades RSTP als Redundanz-Mechanismus aktiviert werden soll, muss zuvor die Large-Tree-Support-Option auf allen Geräten eingeschaltet werden.
– Es wird empfohlen, Large-Tree-Support in Netzen mit weniger als sieben Switches entlang des relevanten Pfades nicht zu aktivieren.

5.2.5.2 Beispieltopologien

5.2.5.3 Redundante Kopplung von Netzsegmenten

In diesem Beispiel sind zwei Netzwerksegmente über redundante Datenpfade mit einander verbunden. Zwei RSTP-Komponenten haben Ports im Zustand „Blocking/Discarding“ (grau hinterlegt). Das ist ausreichend, um das Netzwerk zu betreiben.

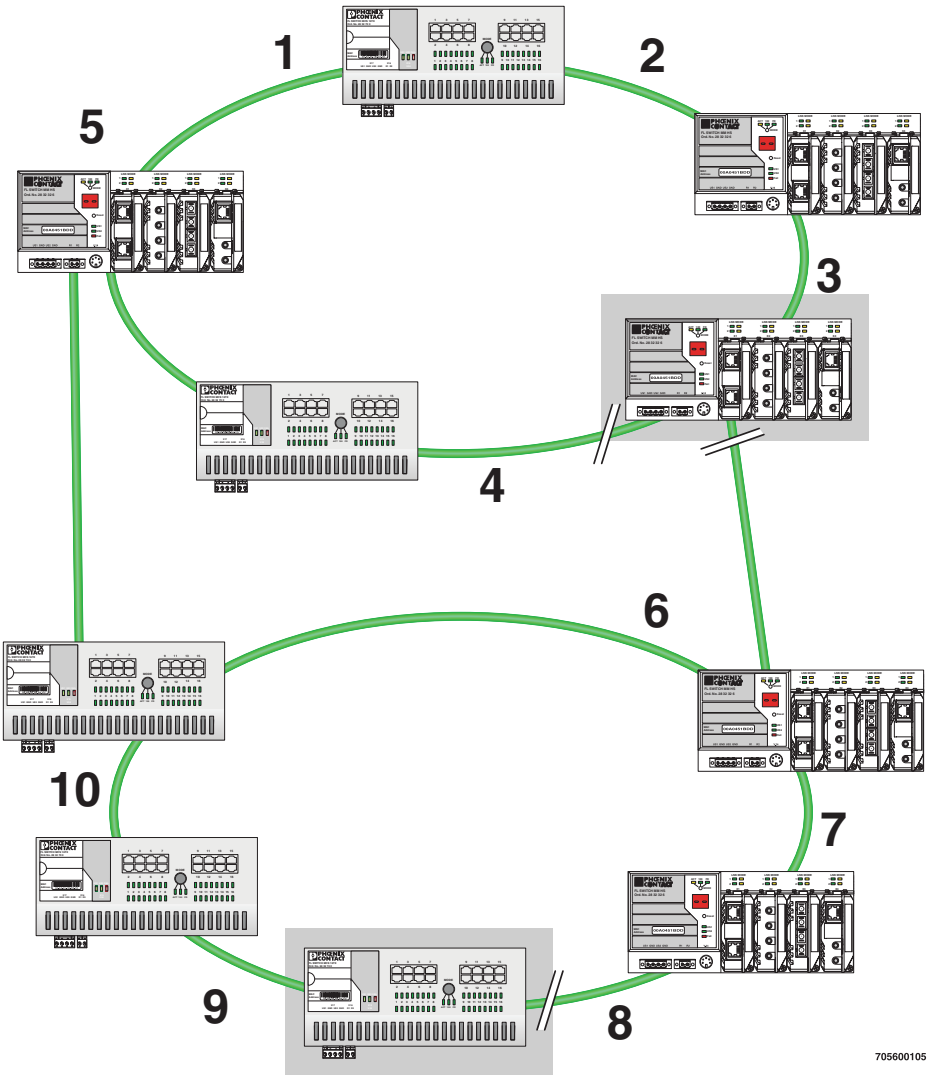


Bild 5-15 Redundante Kopplung von Netzsegmenten

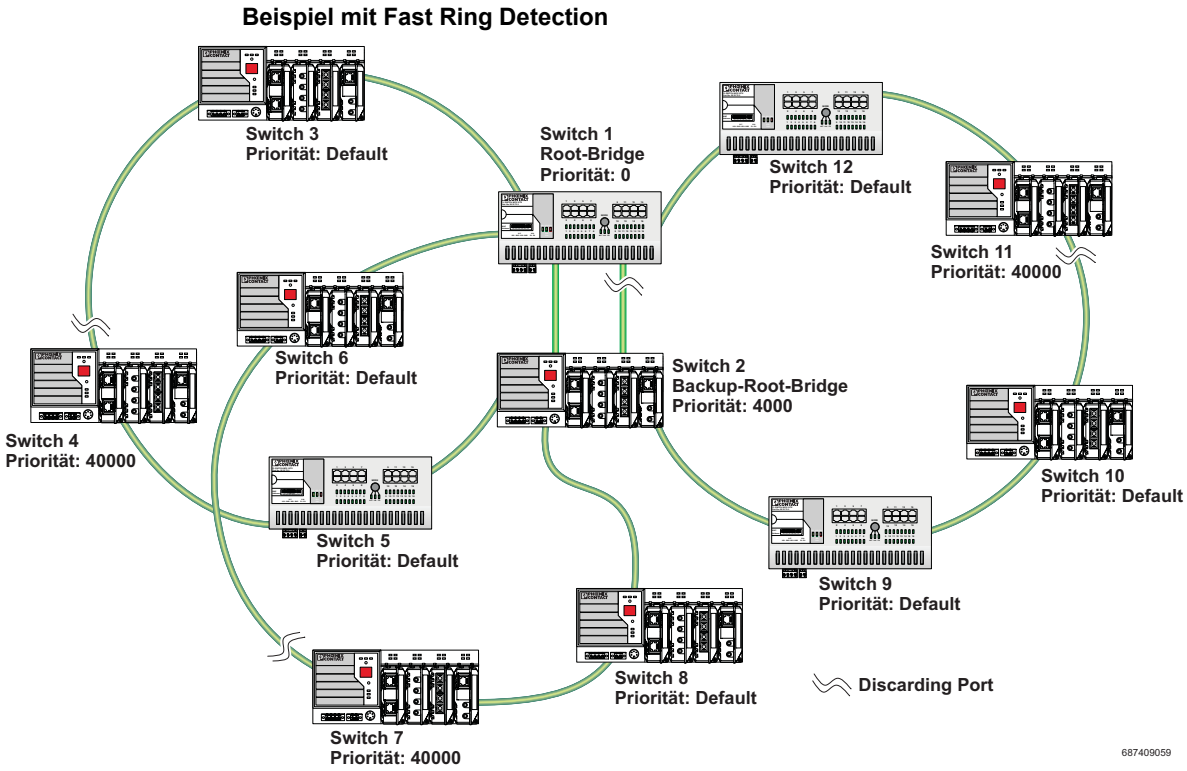


Bild 5-16 Beispiel mit Fast Ring Detection

Die Switches im gezeigten Beispiel sind so angeordnet, dass zwei Geräte an zentraler Position als Root-Bridge und als Backup-Root-Bridge (über die Priorität) konfiguriert werden.

Die niedrigste Priorität bekommt die Root-Bridge, die zweitniedrigste die Backup-Root-Bridge. Die Root- und die Backup-Root-Bridge werden redundant miteinander verbunden. Die verbleibenden Switches werden ringförmig in mehreren Ringen vernetzt. Die Endpunkte der Ringe werden jeweils auf die Root-Bridge und auf die Backup-Root-Bridge geführt. Der aus Sicht der Root-Bridge entfernteste Switch bekommt eine niedrigere Priorität als die Default-Einstellung, z. B. 40000.

Der Vorteil dieser Konstellation ist, dass die einzelnen Ringe sich im Fehlerfall nicht negativ beeinflussen.

5.2.5.4 Funktionsweise des Spanning Tree Protokolls(STP)

Bestandteile einer Spanning-Tree-Domäne

Designated-Switch

Der Switch, der ein bestimmtes LAN-Segment (mit den geringsten Wegekosten) mit dem Root-Switch verbindet.

Der Root-Port

Die anderen Switches setzen den Port mit den geringsten Wegekosten (oder mit der höchsten Gesamtübertragungsgeschwindigkeit) zum Root-Switch in den Forwarding-State.

Es gibt immer nur einen Root-Port pro Switch.
Ausnahme: Der Switch unterstützt mehrere Spanning-Tree-Domänen.

Designated-Ports

Ports im Forwarding-State des Designated-Switches.
Es sind die Ports mit dem „besten“ Weg zum Root-Switch.

Switch-ID

Priorität und MAC-Adresse

Der Switch mit dem niedrigsten Bridge-Identifier bildet den Root-Switch. Der Bridge-Identifier setzt sich aus der MAC-Adresse und der Priorität zusammen. Da die Priorität der MAC-Adresse vorangestellt wird, kann über die Vergabe einer geeigneten Priorität der Root-Switch eindeutig und unabhängig von der MAC-Adresse bestimmt werden. Der Switch mit der höchsten Priorität (kleinster Zahlenwert) wird zum Root-Switch.
Für jeden Switch-Port im Netzwerk wird eine eindeutige Kostenkalkulation erstellt. Diese Root-Pfad-Kosten errechnen sich aus der Summe aller Wegekosten, die für ein Paket auf dem Weg zwischen dem Root-Switch und dem entsprechenden Switch-Port anfallen. Bei einem Switch wird immer der Port mit den geringsten Root-Wegekosten als aktiver Port genutzt. Errechnen sich für zwei oder mehrere Ports die gleichen Root-Wegekosten, so entscheidet die Switch-Priorität und im Weiteren die Port-Priorität über die Wertigkeit des Pfades.

Port-ID

Der Port-Identifier setzt sich aus den Pfadkosten und der Priorität zusammen. Da die Priorität den Pfadkosten vorangestellt wird, kann über die Vergabe einer geeigneten Priorität der Root-Port eindeutig und unabhängig von den Pfadkosten bestimmt werden. Der Port mit der höchsten Priorität (kleinster Zahlenwert) wird zum Root-Port.

5.2.5.5 Abläufe im Spanning Tree Protokoll (STP)

Auswahl des Root-Switches

Bei jeder Topologie-Änderung nimmt jeder Switch zunächst an, dass er selbst der Root-Switch ist und sendet die eigene Switch-ID (z. B. die MAC-Adresse) ins Netz. Alle Switches erhalten diese Nachrichten (MAC-Multicast) und speichern den Inhalt der jeweils „besten“ Nachricht. Die „beste“ Nachricht besteht aus folgenden Topologie-Informationen: Den Root-ID-Informationen und den Kosteninformationen.

Nach dem Empfang der Root-ID-Informationen wird der Switch folgende Vergleiche anstellen:

– Wenn die neue Root-ID eine höhere Priorität hat, als bereits gespeicherte IDs (inklusive der eigenen ID), wird sie gespeichert.
– Ist die Root-ID gleich der bereits gespeicherten, werden die Wegekosten geprüft. Sind sie geringer, wird die ID gespeichert.
– Sind die Root-ID und die Kosten gleich, wird die ID des Absenders geprüft, ist sie niedriger als die eigene, wird sie gespeichert.
– Sind Root-ID, Kosten und Absender-ID gleich, entscheidet die Priorität des Absenderports.

Auswahl eines Designated Switches

Für jedes Netzwerk wird der Switch mit dem günstigsten Root-Anschluss gewählt, dieser Switch wird als Designated-Switch bezeichnet.
Der Root-Switch ist der Designated-Switch für alle direkt angeschlossenen Netzwerke.

Auswahl eines Root-Ports

Nachdem durch Bearbeiten der Root-IDs der Root-Switch bestimmt wurde, legen die Switches jetzt die Root-Ports fest.

Durch die Minimierung aller Anschlusskosten auf dem Weg zum Root-Switch wird der günstigste Pfad bestimmt. Dabei können auch Übertragungsgeschwindigkeiten als Kosten dienen. Beim Switch sind die Pfadkosten, die jeder Port für einen HOP (Sprung eines Datenpaketes von einem Punkt zum nächsten) aufaddiert, auf den Wert 19 (Werkseinstellung/Empfehlung für 100 MBit/s) voreingestellt und können jederzeit vom Benutzer geändert werden.

Auswahl eines Designated Ports

An jedem „Designated Switch“ wird der Port, der die kostengünstigsten Datenverbindung in Richtung Root-Switch liefert, als Designated-Port bezeichnet.

Port-Kosten

Die Port-Kosten können nach zwei verschiedenen Standards eingestellt werden, zum einen nach 802.1D (STP), oder zu anderen nach 801.1W (RSTP).

Falls Sie neben den Geräten von Phoenix Contact Geräte anderer Hersteller benutzen, ist die Einstellung der Port-Kosten nach einem einheitlichen Standard empfehlenswert.

Mit dem SNMP-Objekt „dot1dstpPathCostDefault“ (OID 1.3.6.1.2.1.17.2.18) können Sie den verwendeten Standard umstellen.

Tabelle 5-2 Port-Kosten nach 802.D

Übertragungsrate	Empfohlener Wert	Empfohlener Bereich
10 MBit/s	100	50 - 600
100 MBit/s	19	10 - 60

Tabelle 5-3 Port-Kosten nach 802.W

Übertragungsrate	Empfohlener Wert	Empfohlener Bereich
10 MBit/s	2 000 000	200 000 - 20 000 000
100 MBit/s	200 000	20 000 - 2 000 000

5.2.5.6 Ablaufdiagramm zur Bestimmung des Root-Pfades

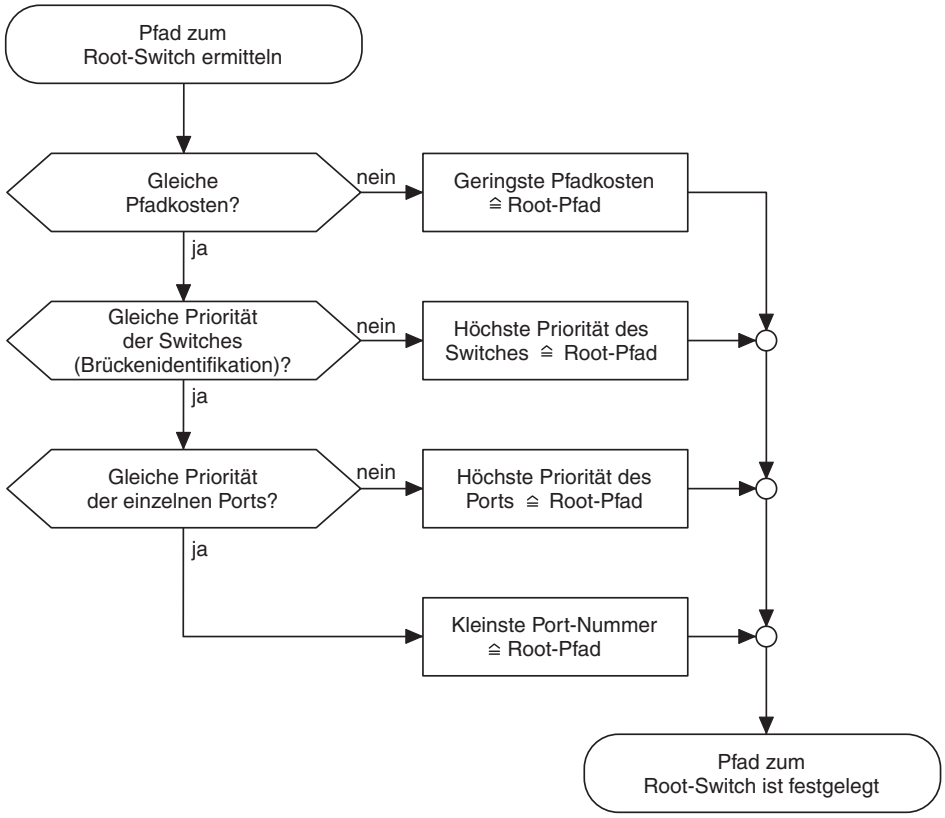


Bild 5-17 Ablaufdiagramm zur Bestimmung des Root-Pfades

5.2.5.7 Erweiterte Konfiguration

Es kann sinnvoll sein, die Topologie, die sich durch das Spanning-Tree-Protokoll ausbildet, nicht den zufälligen MAC-Adressen der beteiligten Switches zu überlassen, sondern diese aktiv vorzugeben.
So kann man beispielsweise Einfluss auf die nicht-/blockierenden Datenpfade nehmen und somit eine Lastverteilung vorgeben.
Ebenso kann es sinnvoll sein, an Ports, die nicht am Spanning Tree teilnehmen, das Spanning-Tree-Protokoll für diese Ports explizit abzuschalten, um von der Fast-Forwarding-Funktion zu profitieren.
Das Spanning-Tree-Protokoll muss auch dann an einzelnen Ports abgeschaltet werden, wenn über diese Ports zwei verschiedene Netzsegmente, die beide Spanning Tree verwenden, gekoppelt werden sollen, ohne dass die beiden Baumstrukturen zu einem großen Spanning Tree verschmelzen.

Festlegen des Root-Switches

Der Root-Switch wird über die Vergabe einer geeigneten Priorität für das Spanning-Tree-Segment vergeben. Stellen Sie auf der Seite „STP Bridge Configuration“ im WBM bei dem Switch, den Sie als Root-Switch vorgesehen haben, die höchste Priorität (kleinster Zahlen-

wert) im Feld „Priority“ ein. Stellen Sie sicher, dass alle anderen Switches des Netzwerks eine kleinere Priorität (größerer Zahlenwert) haben. Die eingestellten Pfadkosten werden hierbei nicht bewertet.

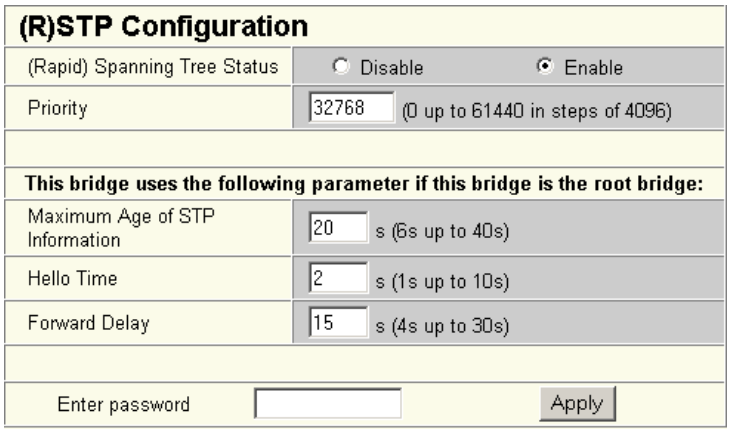


Bild 5-18 Festlegen der Priorität des Root-Switches

Festlegen des Root- oder Designated-Ports

Der Root-Port und der Designated-Port sind immer die Ports, die die geringsten Pfadkosten ausweisen. Bei Kostengleichheit entscheidet die Priorität. Ist auch die identisch, entscheidet die Portnummer. Stellen Sie auf der Seite „STP Port Configuration“ im WBM bei dem Port, den Sie als Root- oder Designated-Port vorgesehen haben, eine geeignete Kombination aus Kosten und Priorität ein. Stellen Sie sicher, dass alle anderen Switches des Netzwerks höhere Kosten oder eine kleinere Priorität (größerer Zahlenwert) haben.

5.2.5.8 Abschalten des Spanning-Tree-Protokolls / Nutzung der Fast-Forwarding-Funktion

Um das Spanning-Tree-Protokoll für einen Port abzuschalten, muss eine der folgenden Bedingungen erfüllt sein:

– An dem Port ist ein Endgerät angeschlossen.
– An dem Port sind weitere Infrastrukturkomponenten angeschlossen, in dem entsprechenden Netzsegment befinden sich keine Loops.
– An dem Port sind weitere Infrastrukturkomponenten angeschlossen, die einen eigenen Spanning Tree bilden. Zu diesem Netzsegment darf keine weitere redundante Verbindung bestehen.

5.2.5.9 Änderung der Protokoll-Timer

Eine Änderung der Protokoll-Timer kann zu instabilen Netzwerken führen.

Sollen z. B. mehr als zehn aktive Spanning-Tree-Komponenten in einem Netzwerk vorhanden sein, kann es erforderlich sein, die Protokoll-Timer zu verändern. Ebenso kann man versuchen, durch eine Änderung der Timer die Rekonfigurationszeiten zu verkürzen. Dies sollte jedoch nur vorsichtig geschehen, um instabile Netze zu vermeiden.
Beachten Sie, dass die Protokollzeiten vom Root-Switch vorgegeben werden und mittels BPDU an alle Teilnehmer verteilt werden. Somit reicht es also zunächst aus, die Werte nur im Root-Switch zu ändern. Fällt der Root-Switch aus, so werden die Timer-Werte eines anderen aktiven STP-Switches (des neuen Root-Switches) für das gesamte Netzsegment gültig. Bitte beachten Sie das bei der Konfiguration Ihrer Komponenten.

Regelung zum Einstellen der Timer-Werte (STP und RSTP)

– Maximale Anzahl der aktiven Spanning-Tree-Komponenten entlang eines Pfades von dem Root-Switch aus (siehe nachfolgende zwei Beispielgrafiken):
  = (MaxAge / 2) - Hello Time +1
– 2 x (Forward Delay - 1 s) ≥ MaxAge
– MaxAge ≥ 2 × (HelloTime + 1 s)

Der Wert ((MaxAge / 2) - Hello Time) für eine Ring-Topologie entspricht der maximalen Anzahl an Komponenten mit aktivem Spanning Tree.

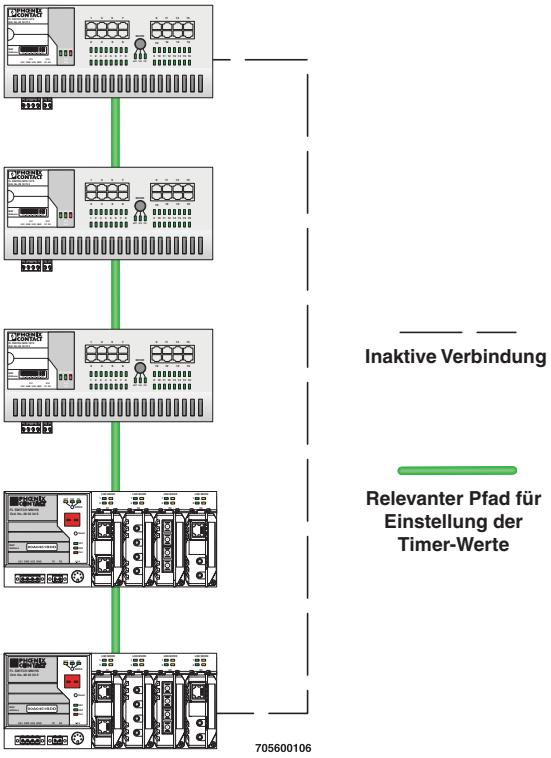


Bild 5-19 Beispiel 1 für den „Relevanten Pfad“

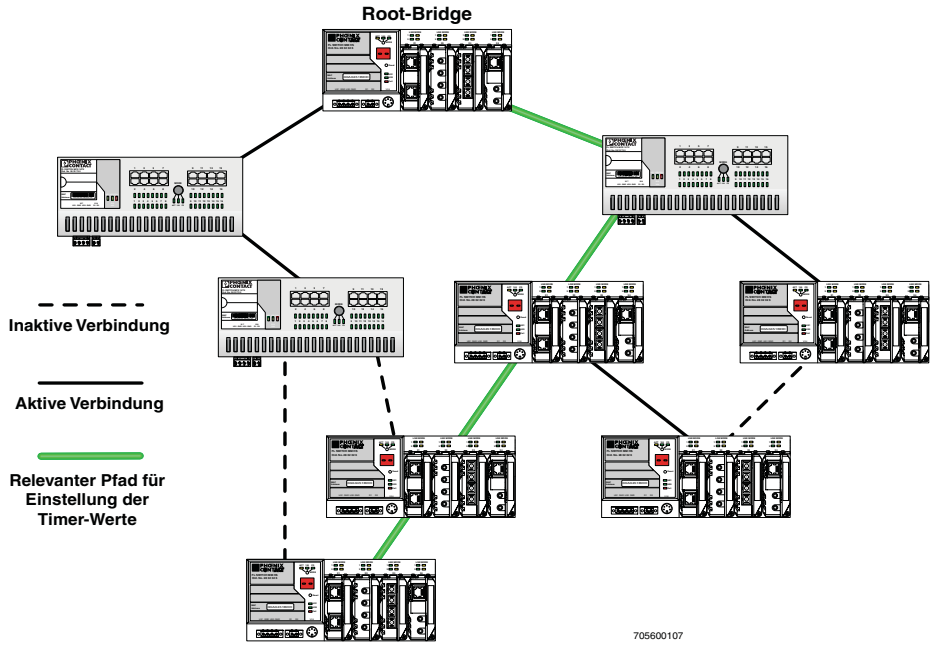


Bild 5-20 Beispiel 2 für den „Relevanten Pfad“

5.2.5.10 Rekonfigurationszeiten

Die Rekonfigurationszeit für einen Spanning Tree hängt von den Timer-Werten für MaxAge und ForwardDelay ab.

Die Rekonfigurationszeit beträgt minimal:
2 × Forward Delay

Die Rekonfigurationszeit beträgt maximal:
2 × ForwardDelay + MaxAge

Bei den in der IEEE-Norm empfohlenen Werten ergibt sich bei zehn aktiven STP-Switches entlang eines Pfades vom Root-Switch aus ein Wert zwischen 30 s und 50 s.

Zu erwartendes Umschalt-Zeitverhalten bei RSTP und RSTP mit aktivierter Ring Detection

Bei der Verwendung von **RSTP** sind Umschaltzeiten im Bereich von **100 ms bis zu 2 s** zu erwarten.

Bei Verwendung der **Fast Ring Detection** sind Umschaltzeiten im Bereich von **100 ms bis zu 500 ms** zu erwarten.

Port-Rollen

Der **Root-Port** eines Switches verbindet diesen Switch, direkt oder über einen anderen Switch (Designated Switch), mit dem Root-Switch.

Der **Designated-Port** ist der Port an einem Designated-Switch, der mit dem Root-Port des nächsten Switches verbunden ist.

An einen **Edge-Port** sind keine weiteren Switches/Bridges mehr angeschlossen. An einen Edge-Port werden Endgeräte angeschlossen.

Ein **Alternate-Port** stellt einen Weg zur Root dar, der aber nicht zum Root-Port wurde. Das heißt, dieser Port nimmt nicht an der aktiven Topologie teil.

6 Medien-Redundanz-Protokoll - MRP

6.1 Allgemeine Funktion

Loops

Mit Hilfe des MRP kann ein Ring im Netzwerk aufgebaut und somit eine redundante Verbindung bereitgestellt werden. Jeder Ring muss einen MRP-Manager enthalten, alle weiteren Teilnehmer (des Ringes) müssen die MRP-Client Funktionalität unterstützen. Der Ring wird über dedizierte Ports aufgebaut. Die MRP-Ports sind im Management des Switches zu konfigurieren. Bei korrekter Konfiguration bietet das MRP eine garantierte maximale Umschaltzeit von 200ms.

Aufgrund des flexiblen Aufbaus des MMS ist es möglich, die zwei erforderlichen MRP-Ports auf verschiedenen Interface-Modulen zu konfigurieren und somit alle Übertragungsmedien für MRP zu nutzen. Die erforderliche MRP-Manager-Lizenz ist im Interface-Modul „FL IF MEM 2TX-D/MRM“ (Art.-Nr. 2891770) enthalten.

Beachten Sie, dass im Auslieferungszustand MRP abgeschaltet ist.

6.2 Die MRP-Lizenz

Die MRP-Lizenzierung erfolgt beim MMS mit Hilfe eines Interface-Moduls. Da die Lizenz an ein austauschbares Modul gebunden ist, sind folgende Möglichkeiten gegeben:

– Ist kein Lizenz-Modul vorhanden, wird die Betriebsart „MRP-Manager“ nicht angeboten oder kann nicht angewählt werden.
– Wird ein Lizenz-Modul während der Laufzeit gesteckt oder ist dieses schon während des Boot-Vorgangs vorhanden, wird die Betriebsart „MRP Manager“ in den User-Interfaces angeboten oder akzeptiert.
– Ist ein Lizenz-Modul während des Boot-Vorgangs vorhanden und ist in der abgespeicherten Konfiguration des MMS die Betriebsart „MRP Manager“ aktiviert, wird die MRP-Manager-Funktion automatisch eingeschaltet.
– Ist während des Boot-Vorgangs kein Lizenz-Modul vorhanden und ist in der gespeicherte Konfiguration der MRP-Manager eingeschaltet, aktiviert das Gerät einen „Sicheren Zustand“, in dem einer der Ring-Ports in den Blocking-Mode gesetzt wird, um eine Schleifenbildung zu vermeiden. Es erscheint die Fehlermeldung, wie sie auch bei einem Ringfehler angezeigt werden würde, um den Benutzer auf diese Fehlkonfiguration hinzuweisen. Nach hinzufügen des Lizenz-Moduls, kann der Manager manuell wieder eingeschaltet oder ein Reboot ausgeführt werden.
– Wird ein Lizenz-Modul während der Laufzeit entnommen, steht die Auswahl des MRP-Managers nicht mehr zur Verfügung.
– Wird ein Lizenz-Modul während der MRP-Manager aktiv ist entnommen, bleibt der Mode solange eingeschaltet, bis das Gerät neu gestartet wird oder ein anderer Mode (MRP Client, Disabled) gewählt wird.

6.2.1 Netzwerkbeispiele

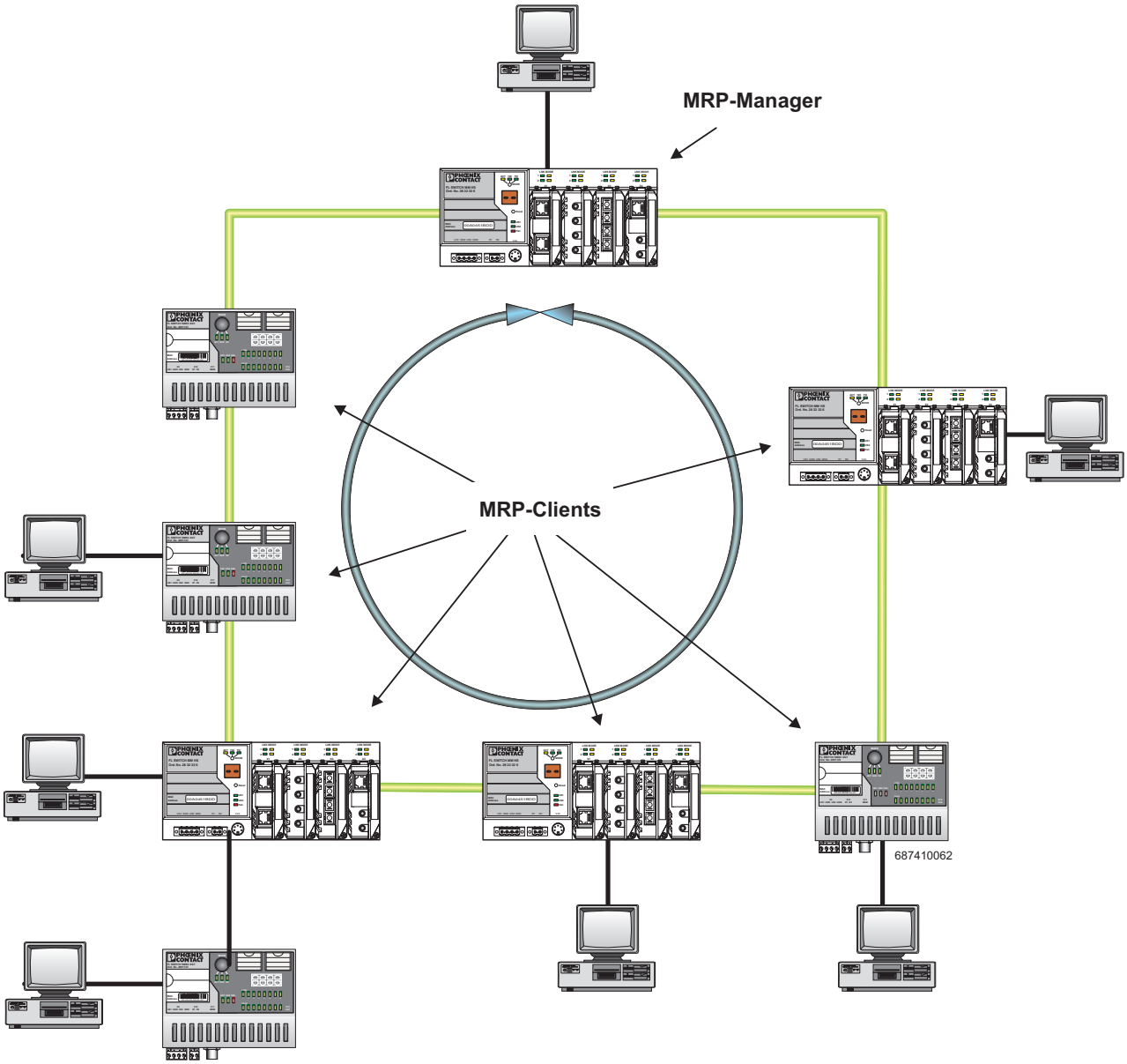


Bild 6-1 Beispiel für einen MRP-Ring

Stellen Sie sicher, dass in der verwendeten Topologie keine ungültige Vermischung von RSTP und MRP stattfindet, z. B. indem zwei der verwendeten Geräte noch einmal **zusätzlich** durch eine RSTP-Verbindung redundant gekoppelt werden.

6.2.1.1 Beispiel für ein zulässiges Netzwerk mit MRP und (R)STP

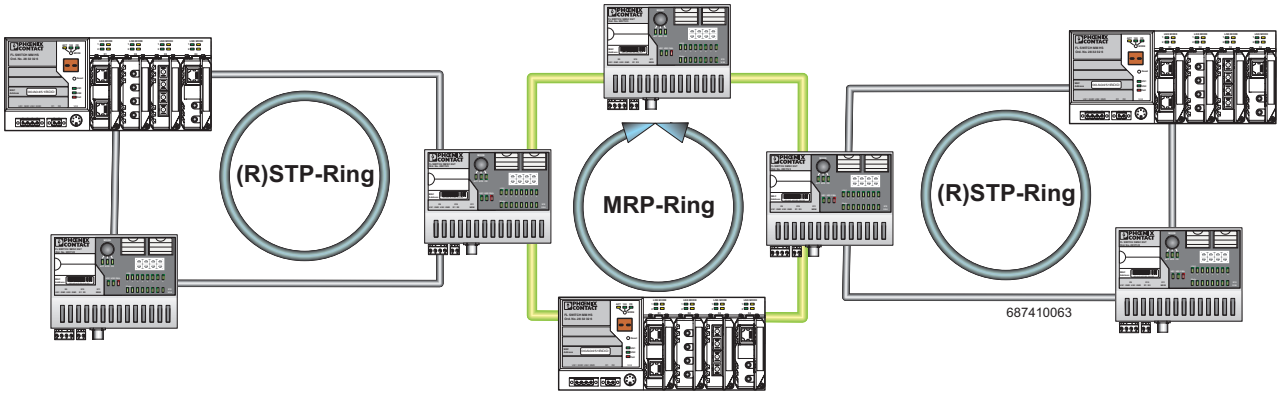


Bild 6-2 Zulässiges Beispiel für MRP mit (R)STP

6.2.1.2 Beispiel für ein nicht zulässiges Beispiel mit MRP und (R)STP

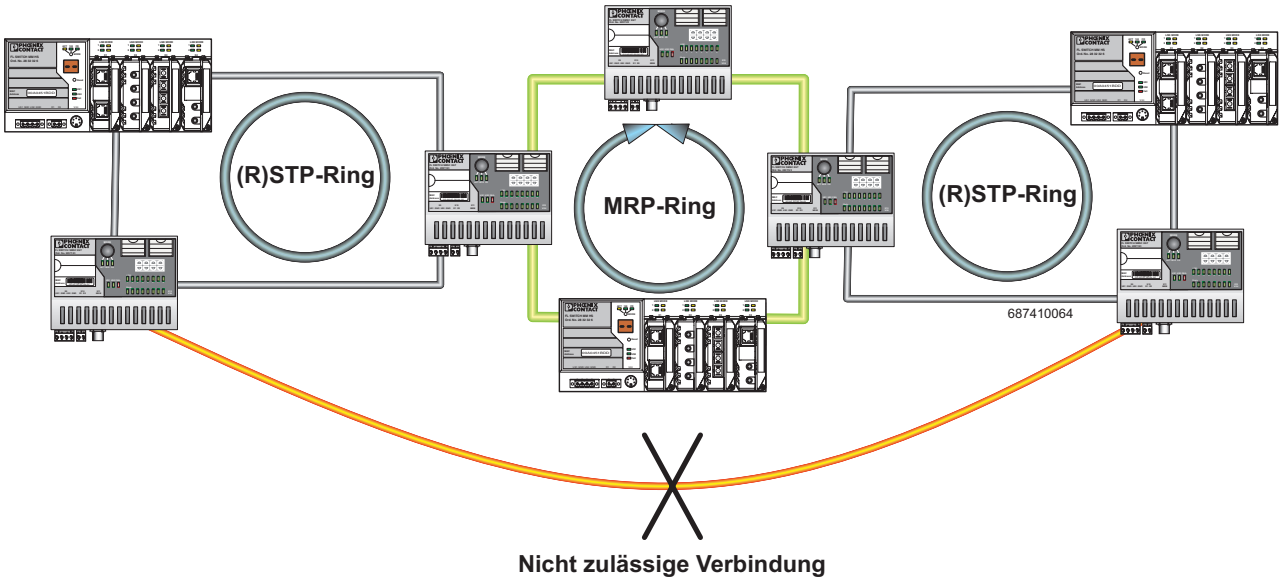


Bild 6-3 Nicht zulässiges Beispiel

6.3 Freischalten der Webseiten zur Nutzung von MRP im WBM

Starten Sie das WBM der Switches, z. B. mit dem Factory Manager, wechseln Sie im Menü „General Configuration“, dann auf die Seite „User Interfaces“. Aktivieren Sie „Redundancy“ und bestätigen Sie mit Ihrem Passwort.

Mit der Aktivierung von „Redundany“ unter „General Configuration/User Interfaces“ ist keiner der Redundanzmechanismen aktiviert. Es wird im WBM-Menü die Seite „Media Redundancy“, unter dem die Funktion konfiguriert und aktiviert werden kann, freigeschaltet.

6.4 Konfiguration von MRP

6.4.1 MRP General

Die Webseite „MRP General“ zeigt die aktuellen Parameter bei der Nutzung des Protokolls. Folgende Informationen werden angezeigt:

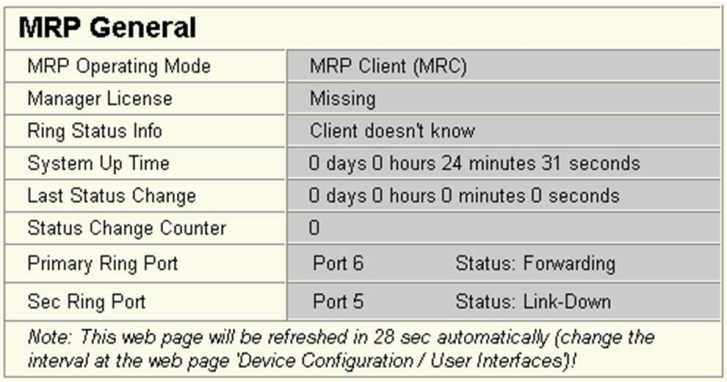
– Operating Mode (Disabled, MRP Client oder MRP Manager)
– Lizenzschlüssel (Present oder Missing)
– Ring-Status, sofern der Switch als MRP-Manager, betrieben wird (OK (Ring geschlossen) oder Fail (Ring offen))
– Topologie-Änderungs-Zähler
– Zeitpunkt der letzten Topologie-Änderung
– Ring-Port-Nummern und Status der Ports (Forwarding oder Blocking)

MRP General

MRP Operating Mode	MRP Manager (MRM)	
Manager License	Present	
Ring Status Info	Ring closed (OK)	
System Up Time	0 days 1 hours 14 minutes 25 seconds	
Last Status Change	0 days 0 hours 31 minutes 27 seconds	
Status Change Counter	17	
Primary Ring Port	Port 6	Status: Forwarding
Sec Ring Port	Port 5	Status: Blocking

Note: This web page will be refreshed in 29 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces)!

Bild 6-4 Webseite „MRP General“ eines MRP-Managers



MRP General

MRP Operating Mode	MRP Client (MRC)	
Manager License	Missing	
Ring Status Info	Client doesn't know	
System Up Time	0 days 0 hours 24 minutes 31 seconds	
Last Status Change	0 days 0 hours 0 minutes 0 seconds	
Status Change Counter	0	
Primary Ring Port	Port 6	Status: Forwarding
Sec Ring Port	Port 5	Status: Link-Down

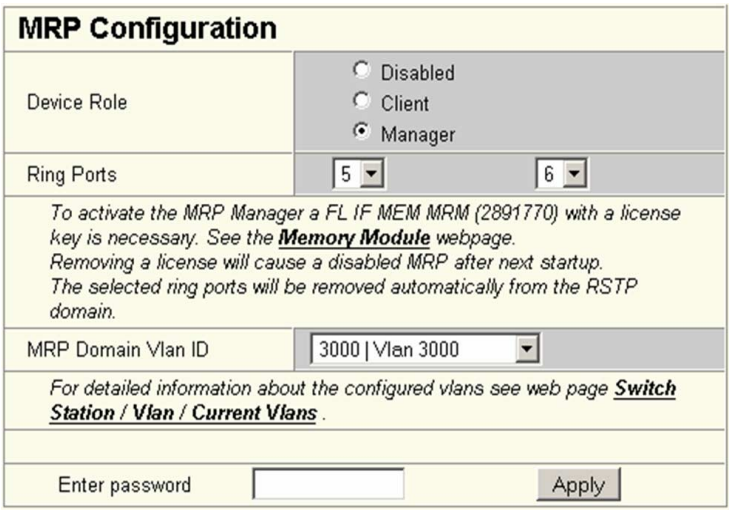
Note: This web page will be refreshed in 28 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces')!

Bild 6-5 Webseite „MRP General“ eines MRP-Clients

6.4.2 MRP Configuration

Die Webseite „MRP Configuration“ ermöglicht die Konfiguration der Protokoll-Parameter. Folgende Parameter werden zur Konfiguration angezeigt:

– Device Role (Disabled, MRP Client oder MRP Manager)
– Auswahl der Ring-Ports, die in den MRP-Ring integriert werden
– Auswahl der VLAN-ID für den Tagging Mode



MRP Configuration

Device Role	○ Disabled ○ Client ◉ Manager
Ring Ports	5 6

*To activate the MRP Manager a FL IF MEM MRM (2891770) with a license key is necessary. See the **Memory Module** webpage.*
Removing a license will cause a disabled MRP after next startup.
The selected ring ports will be removed automatically from the RSTP domain.

MRP Domain Vlan ID	3000 | Vlan 3000

*For detailed information about the configured vlans see web page **Switch Station / Vlan / Current Vlans** .*

Enter password [ ] Apply

Bild 6-6 Webseite „MRP Configuration“

6.4.2.1 Verwendung von MRP im VLAN-Mode

Bei der Verwendung von VLANs wird den MRP-Paketen ein Standard-Tag mit höchster Priorität vergeben. Dazu kann in der MRP-Konfiguration eine VLAN-ID angegeben werden. Es können nur statische VLAN-Einträge, die im WBM unter „Switch/VLAN/Static VLAN“, verwendet werden. Der Tag wird dem MRP-Paket nur dann hinzugefügt, wenn der Port, auf dem das MRP-Paket gesendet wird, im Tagging-Mode betrieben wird.

7 Multicast Filtering

7.1 Grundlagen

Multicast

Multicast-Anwendungen versenden, anders als Unicast-Anwendungen mit einer Punkt-zu-Punkt-Kommunikation, ihre Daten nicht mit der MAC-Adresse des Zieles, sondern mit einer davon unabhängigen Multicast-Gruppen-Adresse. Bei der stets verbindungslosen Kommunikation versendet eine Station **ein** Datenpaket, das von einer oder mehreren Empfänger-Stationen empfangen wird.

Vorteile:

1 Damit z. B. ein Datenpaket eines Senders acht Empfänger erreicht, muss das gleiche Paket nicht achtmal an die Adressen der acht Teilnehmer gesendet werden, sondern nur einmal an die Adresse der Multicast-Gruppe, in der sich die acht Teilnehmer befinden.

2 Durch die Verwendung von Multicast-Kommunikation und Filterung wird der Bedarf an Bandbreite zur Übertragung der Daten reduziert, da jedes Paket nur einmal versendet wird.

Es können maximal 128 Multicastgruppen angelegt werden, davon können maximal 20 Gruppen statische Gruppen sein.

7.2 Freischalten der Webseiten zum Multicast Filtering im WBM

Starten Sie das WBM der Switches, z. B. mit dem Factory Manager, wechseln Sie im Menü „General Configuration“, dann auf die Seite „User Interfaces“. Aktivieren Sie „Multicast Filtering“ und bestätigen Sie mit Ihrem Passwort.

Mit der Aktivierung von „Multicast Filtering “ unter „General Configuration/User Interfaces“ ist der Multicast-Mechanismus **nicht** aktiviert. Es wird im WBM-Menü die Seite „Multicast“, unter dem die Funktion konfiguriert und aktiviert werden kann, freigeschaltet.

7.3 Statische Multicast-Gruppen

Statische Multicast-Gruppen müssen auf jedem Switch manuell angelegt und alle Ports, über die Gruppenmitglieder zu erreichen sind, hinzugefügt werden. Die Vorteile statischer Gruppen sind:

1 Einfache Festlegung der Netzwerkpfade, auf die der Multicast-Datenverkehr bekannter Gruppen beschränkt wird.

2 Kein Querier erforderlich (siehe „Query“ auf Seite 7-7).

Folgende Randbedingungen müssen eingehalten werden:

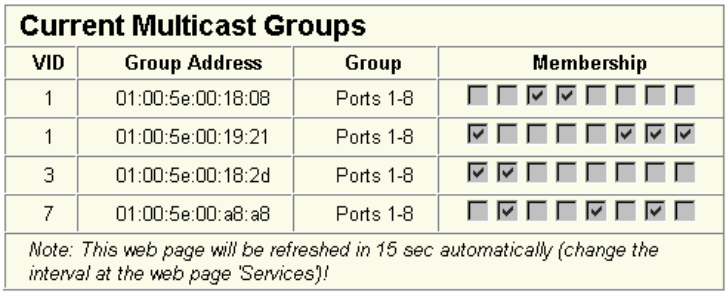
– Genaue Netzwerkdokumentation zur Festlegung der Pfade ist erforderlich.

– Mögliche redundante Pfade durch Spanning Tree müssen bei der Zuordnung der Ports berücksichtigt werden.

– Bei Netzwerkänderung, im Servicefall oder bei Erweiterung müssen die Multicast-Datenpfade wieder hergestellt werden.

7.3.1 Webseite „Current Multicast Groups“

Die Tabelle auf der Webseite bietet eine Übersicht über die aktuell angelegten Multicast-Gruppen auf diesem MMS. Das können Multicast-Gruppen aufgrund von IGMP-Snooping oder statisch angelegte Gruppen sein.



Current Multicast Groups

VID	Group Address	Group	Membership
1	01:00:5e:00:18:08	Ports 1-8	☐ ☐ ☑ ☑ ☐ ☐ ☐ ☐
1	01:00:5e:00:19:21	Ports 1-8	☑ ☐ ☐ ☐ ☐ ☑ ☑ ☑
3	01:00:5e:00:18:2d	Ports 1-8	☑ ☑ ☐ ☐ ☐ ☐ ☐ ☐
7	01:00:5e:00:a8:a8	Ports 1-8	☐ ☑ ☐ ☐ ☑ ☐ ☑ ☐

Note: This web page will be refreshed in 15 sec automatically (change the interval at the web page 'Services')!

Bild 7-1 Webseite „Current Multicast Groups“

Die Checkboxen zeigen, welcher Port der jeweiligen Gruppe zugeordnet ist.

Beachten Sie, dass alle dem Switch bekannten Multicast-Gruppen, also auch die dynamisch erkannten Gruppen, die nicht manuell angelegt wurden, auf dieser Webseite angezeigt werden.

Als Grundlage für die Übersicht der Gruppenzugehörigkeit dient die SNMP-Gruppe „dot1qTpGroupTable“. In dieser Tabelle sind alle Gruppen (statische Einträge und IGMP) mit ihren Gruppenmitgliedern aufgelistet.

7.3.2 Anlegen von statischen Multicast-Gruppen

Diese Webseite dient dem Anlegen und der Verwaltung der statisch konfigurierten Multicast-Gruppen. Um neue Multicast-Gruppen anzulegen, tragen Sie im Feld „Multicast Group Address“ die vorgesehene MAC-Adresse (siehe „Multicast-Adressen“ auf Seite 7-4) der Multicast-Gruppe ein, fügen Sie die Ports der Datenpfade zu den Gruppenmitgliedern hinzu und bestätigen Sie mit Ihrem gültigen Passwort die Eingabe. Falls Sie die Gruppenadresse als IP-Adresse eingeben, wird die IP-Adresse nach den Vorgaben der IEEE 802.1 D/p in eine Multicast-MAC-Adresse umgewandelt.

Das Überschreiben einer dynamischen Gruppe durch eine statische Konfiguration hat zur Folge, dass dynamisch keine neue Port-Zuordnung für diese Gruppe angelegt werden kann. Erst nach dem Löschen der Gruppe kann dynamisch eine Port-Zuordnung für die Gruppe gestartet werden.

Umrechnung

Die Vorschriften zur Umrechnung einer Multicast-IP-Adresse in eine Multicast-MAC-Adresse bedingen eine Abbildung verschiedener IP-Gruppen auf dieselbe MAC-Gruppe. Vermeiden Sie die Verwendung von IP-Gruppen, die sich

– im **ersten und zweiten Byte** von rechts **nicht** unterscheiden und
– im **dritten Byte** von rechts eine Differenz von 128 aufweisen.

Das **vierte Byte** von rechts wird immer durch 01:00:5e bei der Umrechnung ersetzt. Siehe nachfolgendes Beispiel.

Aufgrund der Umrechnung von IP- in MAC-Adressen sollten Sie IP-Adressen vermeiden, die sich im dritten Byte von rechts um 128 unterscheiden. Beispiel:

		3. Byte v. r.	
1. Multicast-IP-Adresse:	228 .	30	. 117 . 216
2. Multicast-IP-Adresse:	230 .	158	. 117 . 216
Differenz:		128	

Beide Multicast-IP-Adressen werden in die Multicast-MAC-Adresse 01:00:5e:1e:75:d8 umgerechnet.

Die Gruppe wird in die Liste der vorhandenen statischen Multicast-Gruppen eingefügt. Diese Liste, die in einer Listbox angezeigt wird, ist über SNMP als „dot1qStaticMulticastTable“ bekannt.

Vorgenommene Einstellungen werden nicht automatisch dauerhaft gespeichert. Eine dauerhafte Speicherung der jetzigen Konfiguration erreichen Sie mit „save current configuration“ auf der Webseite „Configuration Management“.

Zuordnung der Ports

Nachdem Sie eine neue Gruppe in das Feld „Multicast Group Address“ eingetragen haben, fügen Sie die Ports der Gruppenmitglieder durch Auswahl der entsprechenden Checkboxen hinzu und bestätigen Sie mit Ihrem Passwort und „Apply“.

Änderung der Zuordnung

Um die Port-Zuordnung zu ändern oder zu löschen, wählen Sie die entsprechende Gruppe in der Listbox „Select Group“ aus. Die Gruppenmitglieder werden durch markierte Checkboxen angezeigt und können bei Bedarf geändert werden. Eine Aktion wird nach der Passwort-Eingabe mit „Apply“ oder „Delete“ abgeschlossen.

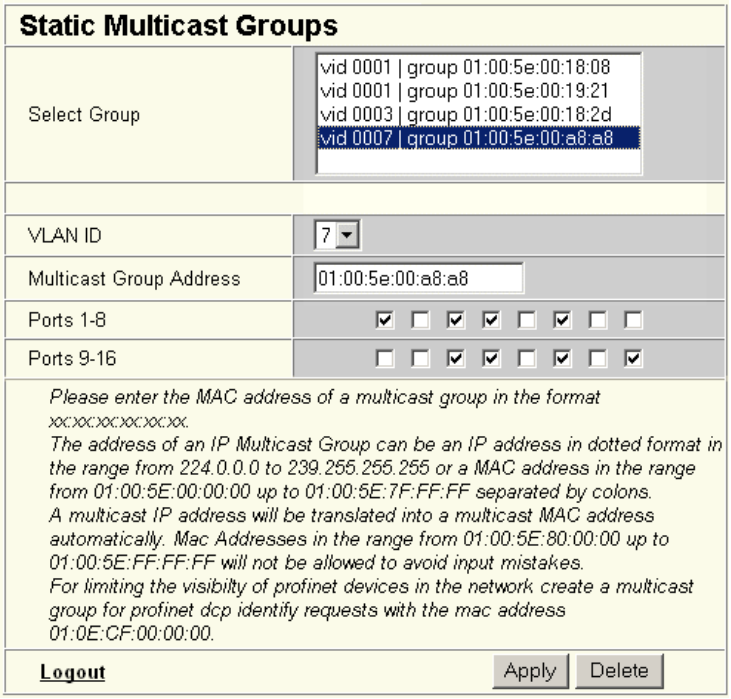

Static Multicast Groups
Select Group
vid 0001 | group 01:00:5e:00:18:08
vid 0001 | group 01:00:5e:00:19:21
vid 0003 | group 01:00:5e:00:18:2d
vid 0007 | group 01:00:5e:00:a8:a8
VLAN ID
7
Multicast Group Address
01:00:5e:00:a8:a8
Ports 1-8
Ports 9-16
Please enter the MAC address of a multicast group in the format xx:xx:xx:xx:xx:xx.
The address of an IP Multicast Group can be an IP address in dotted format in the range from 224.0.0.0 to 239.255.255.255 or a MAC address in the range from 01:00:5E:00:00:00 up to 01:00:5E:7F:FF:FF separated by colons.
A multicast IP address will be translated into a multicast MAC address automatically. Mac Addresses in the range from 01:00:5E:80:00:00 up to 01:00:5E:FF:FF:FF will not be allowed to avoid input mistakes.
For limiting the visibilty of profinet devices in the network create a multicast group for profinet dcp identify requests with the mac address 01:0E:CF:00:00:00.
Logout
Apply
Delete

Bild 7-2 Menü „Static Multicast Groups“

Prüfung der Gruppenzugehörigkeit

Um zu überprüfen, welche Ports welcher Gruppe zugeordnet sind, wählen Sie eine der vorhandenen Gruppen aus. Die zugehörige MAC- Adresse wird dann im Textfeld „Multicast Group Address“ angezeigt. Die Mitglieder der Gruppe werden durch die aktivierten Checkboxen gekennzeichnet.

Multicast-Adressen

Verwenden Sie keine Multicast-MAC-Adressen, die im Bereich von 01:00:5e:80:00:00 bis 01:00:5e:FF:FF:FF liegen.

Falsches Format

Auf ein falsches MAC-Adressenformat und die Eingabe von „Nicht-Multicast-Adressen“ wird hingewiesen und der Eintrag nicht zugelassen.

Beachten Sie, dass bei Multicast-MAC-Adressen die Bytes durch Doppelpunkt (:) und IP-Multicast-Adressen die Bytes durch Punkt (.) getrennt werden.

7.3.3 Vorgehensweise zum Anlegen einer Multicast-Gruppe

Verschaffen Sie sich einen Überblick über die in dem Netzwerk vorhandenen Multicast-Anwendungen und die verwendeten Multicast-Adressen. Legen Sie für jede Multicast-Applikation oder für die verwendete Multicast-Adresse eine Gruppe an und fügen Sie aus der Sicht **jedes** Switches die Ports hinzu, an denen ein Teilnehmer der entsprechenden Gruppe direkt angeschlossen ist oder über den der Teilnehmer zu erreichen ist.

Beispiel

In der folgenden Tabelle sind die Ports (je Switch) mit einem „X“ gekennzeichnet, an denen die Empfänger der Multicast-Daten jeweils angeschlossen sind. Siehe als Beispielkonfiguration Bild 7-3 auf Seite 7-6.

Tabelle 7-1 Zuordnung der Multicast-Ports auf den Switches

	Switch 1	Switch 2	Switch 3	Switch 4	Switch 5	Switch 6	Switch 7
Port 1							
Port 2	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Port 3							
Port 4					**X**		**X**
Port 5				**X**			
Port 6						**X**	
Port 7	**X**						
Port 8			**X**		**X**		

Beachten Sie, dass die möglichen redundanten Pfade bei Verwendung von Rapid Spanning Tree ebenfalls bei der Bildung der Multicast-Gruppen berücksichtigt werden müssen.

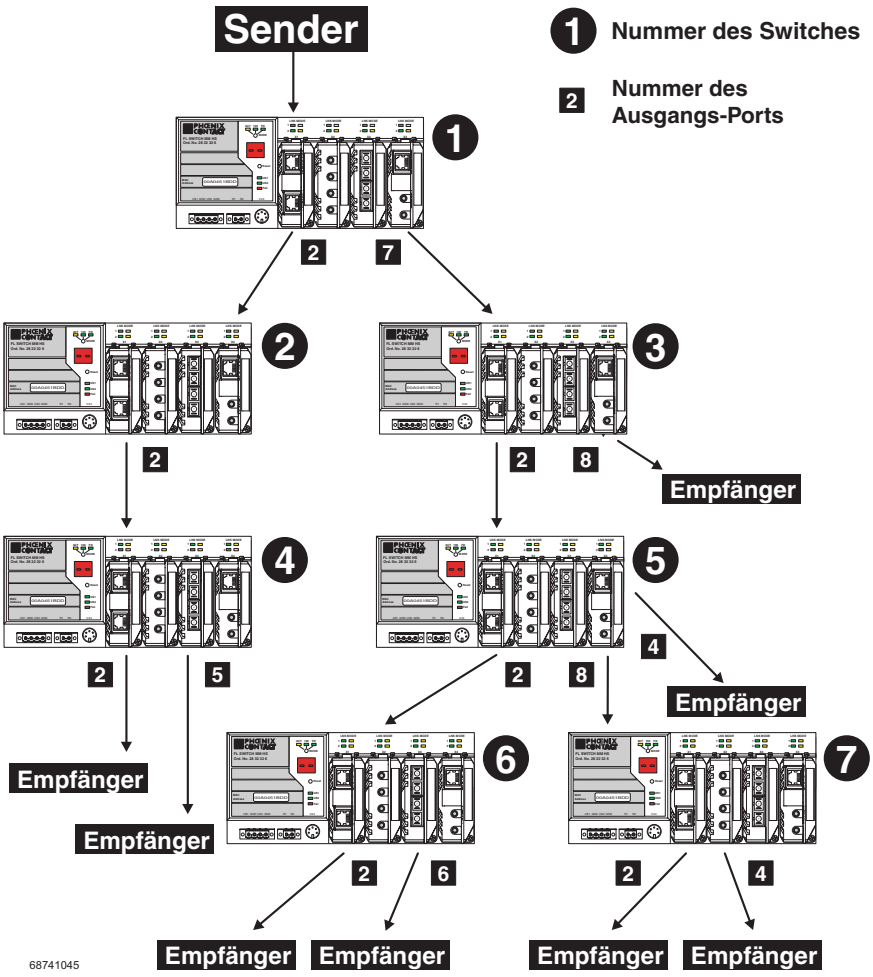


Bild 7-3 Konfigurationsbeispiel

Berücksichtigen Sie der Bildung der Multicast-Gruppen die möglichen redundanten Pfade bei Verwendung von Rapid Spanning Tree

7.4 Dynamische Multicast-Gruppen

7.4.1 Internet Group Management Protocol - IGMP

IGMP auf Layer 3

Das Internet Group Management Protocol beschreibt ein Verfahren zur Verteilung von Informationen über Multicast-Applikationen zwischen Routern und Endgeräten auf IP-Ebene (Layer 3).

Ein Netzwerkteilnehmer versendet beim Start einer Multicast-Anwendung einen sogenannten IGMP Membership Report und gibt damit seine Teilnahme an einer bestimmten Multicast-Gruppe bekannt. Ein Router sammelt diese Membership Reports und pflegt damit die Multicast-Gruppen seines Subnetzes.

Query

In regelmäßigen Abständen versendet der Router IGMP Queries und regt die Teilnehmer mit Multicast-Empfänger-Applikationen zum erneuten Senden eines Membership Reports an.

Die Funktion „IGMP Query“ sendet nur im Management-VLAN und zieht sich nur bei einem besseren Querier im Management VLAN zurück.

Der Router trägt die IP-Multicast-Group-Adresse aus der Report-Nachricht in seine Routing-Tabelle ein. Dies bewirkt, dass er Frames mit dieser IP-Multicast-Group-Adresse im Zieladressfeld ausschließlich gemäß der Routing-Tabelle vermittelt. Geräte, die nicht mehr Mitglied einer Multicast-Gruppe sind, melden sich mit einer Leave-Nachricht ab (ab IGMP Version 2) und versenden keine Report-Nachrichten mehr.
Der Router entfernt den Routing-Tabelleneintrag ebenso, wenn er innerhalb einer bestimmten Zeit (Aging Time) keine Report-Nachricht empfängt. Sind mehrere Router mit aktiver IGMP-Query-Funktion im Netz, dann verhandeln diese untereinander, welcher Router die Query-Funktion übernimmt. Diese Entscheidung wird aufgrund der IP-Adressen gefällt, wobei der Router mit der niedrigeren IP-Adresse weiterhin als Querier fungiert und alle anderen Router keine weiteren Query Messages versenden. Empfangen diese Router für eine gewisse Zeitspanne keine neuen Query-Telegramme, werden sie selber wieder als Querier aktiv. Ist kein Router im Netz, dann kann ein entsprechend ausgestatteter Switch die Query-Funktion übernehmen. Beachten Sie, dass der MMS als IGMP-Querier nur im Management-VLAN arbeitet.

IGMP-Snooping

Ein Switch, der einen Multicast-Empfänger mit einem Router verbindet, kann mit Hilfe des IGMP-Snooping-Verfahrens die IGMP-Informationen mitlesen und auswerten. IGMP-Snooping übersetzt IP-Multicast-Group-Adressen in MAC-Multicast-Adressen, so dass die IGMP-Funktion auch von Layer 2-Switches wahrgenommen werden können. Der Switch trägt die vom IGMP-Snooping aus den IP-Adressen gewonnenen MAC-Adressen der Multicast-Empfänger in die eigene Multicast-Filtertabelle ein. Somit filtert der Switch Multicast-Pakete bekannter Multicast-Gruppen und leitet die Pakete nur an die Ports weiter, an denen entsprechende Multicast-Empfänger angeschlossen sind.

IGMP-Snooping kann auf Layer 2 nur genutzt werden, wenn alle Endgeräte IGMP-Nachrichten senden. Der IP-Stack von Multicast-fähigen Endgeräten, deren Applikationen sich an eine Multicast-Adresse binden, versendet automatisch entsprechende Membership-Reports.

IGMP-Snooping funktioniert unabhängig vom Internet Group Management Protocol (IGMP)!

7.4.1.1 Extended Multicast Filtering

Ist IGMP-Snooping aktiv, werden auch Multicast-Datenströme erkannt, für die keine Membership-Reports von möglichen Empfängern registriert werden. Für diese Multicasts werden dynamisch Gruppen angelegt. Diese Multicasts werden an den Querier weitergeleitet, d. h. der Querier-Port wird in der Gruppe eingetragen.

Ist der Switch selbst der Querier, werden solche Multicasts geblockt.

7.4.2 Webseite „General Multicast Configuration“

Diese Webseite bietet globale Einstellungen zur Multicast-Unterstützung. IGMP-Snooping kann hier aktiviert und eine Aging Time für die IGMP-Snooping-Informationen festgelegt werden.

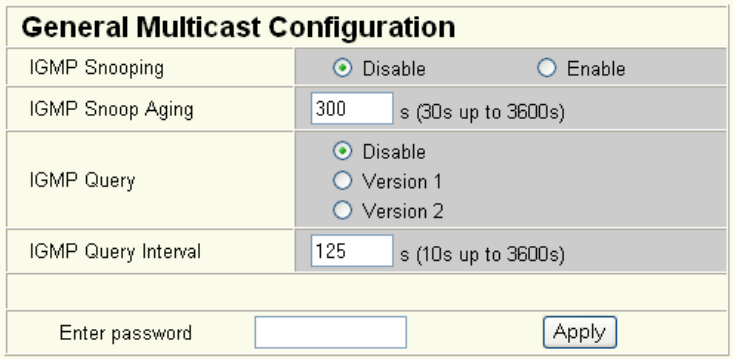


Bild 7-4 Webseite „General Multicast Configuration“

IGMP Snooping
Beim IGMP Snooping hört der Switch die über das Netzwerk gesendeten IGMP-Nachrichten passiv mit und legt dynamisch die entsprechenden Gruppen an. Die Gruppen werden nicht gespeichert und gehen beim Power-Down oder Ausschalten der Snooping-Funktion verloren.

IGMP Query
Ein MMS mit aktivierter Query-Funktion versendet im Abstand „Query Interval“ aktiv Queries und wertet die empfangenen Reports aus. Der MMS versendet IGMP-Query-Reports nur bei eingeschaltetem IGMP-Snooping und nur im Management-VLAN.

8 Virtual Local Area Network - VLAN

8.1 Grundlagen

VLAN

Ein VLAN ist ein in sich geschlossenes Netzwerk, das aber nicht physikalisch, sondern logisch/funktional von anderen Netzwerken getrennt ist. Ein VLAN bildet eine eigene Broadcast- und Multicast-Domain, die nach bestimmten logischen Kriterien vom Anwender definiert wird. Das Ziel beim Einsatz von VLANs ist die Trennung von physikalischer und logischer Netzwerkstruktur:

– Datenpakete werden ausschließlich innerhalb des jeweiligen VLANs weitergeleitet.
– Die Mitglieder eines VLANs können räumlich weit verteilt sein.

Die reduzierte Ausbreitung von Broadcasts und Multicasts steigert die verfügbare Bandbreite innerhalb eines Netzwerksegments. Zusätzlich wird durch die strikte Trennung des Datenverkehrs die Sicherheit erhöht.

Um Datenverkehr zwischen VLANs zu ermöglichen ist ein Router oder ein ähnliches Layer-3-Gerät notwendig.

Die VLANs können beim Switch statisch oder dynamisch angelegt werden. Bei der dynamischen Konfiguration werden die Datenrahmen mit einem sogenannten Tag versehen. Ein Tag ist eine Ergänzung innerhalb des Datenrahmens, der die VLAN-Zugehörigkeit anzeigt. Dieser Tag kann bei entsprechender Konfiguration bei der Übertragung vom ersten Switch der Übertragungskette hinzugefügt und vom letzten wieder entfernt werden. Mehrere unterschiedliche VLANs können daher die gleichen Switches/Infrastrukturkomponenten verwenden. Alternativ ist auch der Einsatz von Endgeräten möglich, die VLAN-Tags unterstützen.

8.2 Freischalten der VLAN-Webseiten im Web Based Management

Starten Sie das Web Based Management der Switches, z. B. mit dem Factory Manager, wechseln Sie im Menü „General Configuration“, dann auf die Seite „User Interfaces“. Aktivieren Sie die Funktion „VLAN“ und bestätigen Sie mit Ihrem Passwort.

Mit der Aktivierung von „VLAN“ unter „User Interfaces“ ist der VLAN-Mechanismus **nicht** aktiviert. Es wird im WBM-Menü die Seite „VLAN“, unter dem die Funktion konfiguriert und aktiviert werden kann, freigeschaltet.

Mit der Deaktivierung der VLAN-Konfigurationsseiten unter „User Interfaces“ ist der VLAN-Mechanismus **nicht** deaktiviert. Die gespeicherte VLAN-Konfiguration bleibt erhalten.

8.2.1 Management VLAN-ID

Das Management des Switches ist im Auslieferungszustand dem VLAN 1 zugeordnet. Außerdem sind alle Ports im Auslieferungszustand dem VLAN 1 zugeordnet. Somit ist sichergestellt, dass über alle Ports die netzwerkgestützten Management-Funktionen zu erreichen sind.

Stellen Sie sicher, dass das Management des MMS sich immer in einem VLAN befindet, auf das Sie auch Zugriff haben.

Die VLAN-ID 1 kann nicht gelöscht werden und ist somit immer auf dem Switch angelegt.

Wenn Sie das VLAN löschen, in dem sich das Management des MMS befindet, wird das Management automatisch ins VLAN 1 gelegt.

Die Funktion „IGMP Query“ sendet nur im Management-VLAN und zieht sich nur bei einem besseren Querier im Management VLAN zurück.

8.2.2 Änderung der Management VLAN-ID

8.2.2.1 Konfiguration im Transparent Mode

1. Schalten Sie im WBM die Seiten zur VLAN-Konfiguration frei (WBM: User-Interfaces/Virtual LAN).
2. Legen Sie auf der Webseite „Static VLANs“ die erforderlichen VLANs an.
3. Ordnen Sie nun auf der Webseite „VLAN Port Cfg. Table“ die Ports für eingehende Pakete den einzelnen VLANs mittels der VLAN ID zu.
4. Auf der Webseite „IP Configuration“ können Sie jetzt die gewünschte Management VLAN-ID einstellen.
5. Schalten Sie jetzt auf der Webseite „General VLAN Configuration“ den Switch in den VLAN-Mode „Tagging“.
6. Speichern Sie die Konfiguration auf der Webseite „General Configuration/Config Management“ und starten Sie anschließend den Switch neu.

8.2.2.2 Konfiguration im Tagging Mode (wird in der Regel benutzt, um die Management VLAN-ID bei einer bestehenden VLAN-Konfiguration zu ändern)

1. Verbinden Sie den PC direkt mit dem zu konfigurierenden Switch über einen Port (A), dessen VLAN ID auf „1“ steht.
2. Führen Sie jetzt ein Firmware-Update auf eine Firmware größer 4.03 durch und starten Sie den Switch neu.
3. Legen Sie jetzt einen anderen Port (B) in das gewünschte Management VLAN. Dieser Port B muss „Untagged Member“ des gewünschten Management VLANs sein. Stellen Sie ggfs. die Port VLAN-ID entsprechend ein.
4. Stellen Sie die gewünschte VLAN-ID als Management VLAN ein.
5. Verbinden Sie jetzt Ihren PC über den Port B mit dem Switch und speichern die Konfiguration.

8.3 General VLAN Configuration

Auf der Webseite „Switch Station/VLAN/General VLAN Configuration“ können grundlegende Einstellungen zum VLAN-Betrieb gemacht werden.

Transparent

Im „Transparent“-Modus verarbeitet der Switch die eingehenden Datenpakete so wie im Kapitel Frame-Switching beschrieben (siehe Kapitel 3.3 auf Seite 3-30). Die Datenpakete werden weder in ihrer Struktur, noch in ihrem Inhalt verändert. Die Information über die VLAN-Zugehörigkeit aus einem evtl. im Datenpaket enthaltenem Tag wird ignoriert.

Tagging

Im „Tagging“-Modus werden eingehende Pakete entsprechend den festgelegten VLAN-Regeln angenommen, ein VLAN-Tag wird bei Bedarf eingefügt und entsprechend den Informationen aus dem Tag vom Switch und auch dem Management bearbeitet. Beim Versenden der Ethernet-Pakete berücksichtigt der Switch die vorgegebenen Regeln für das jeweilige VLAN oder den jeweiligen Ausgangs-Port.

Die Management VLAN-ID gibt an, in welchem VLAN der Switch selber zu erreichen ist, wenn er im VALN-Modus „Tagging“ arbeitet.

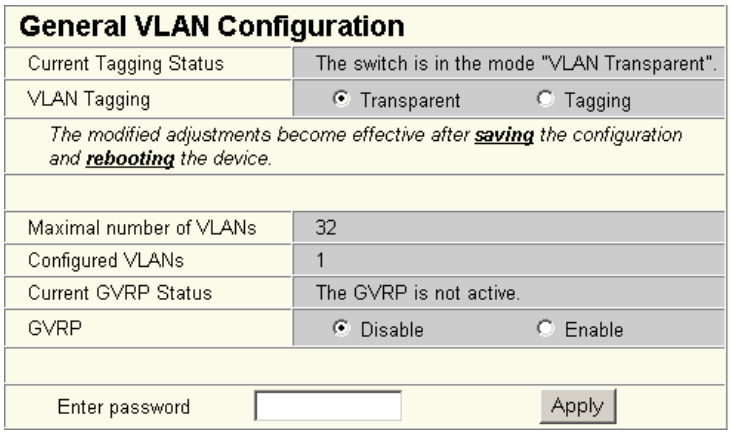


Bild 8-1 Menü „General VLAN Configuration“

Der Switch unterstützt maximal 32 verschiedene VLANs.

Nach dem Umschalten des VLAN-Modus von „Tagging“ auf „Transparent“ oder umgekehrt, ist es notwendig, die aktuelle Konfiguration zu speichern und einen Reset des Gerätes auszulösen, damit die Änderung aktiv wird. Der aktuell gültige Zustand kann in der Zeile „Current Tagging Status“ abgelesen werden.

GVRP-Protokoll

Das GVRP-Protokoll (GARP VLAN Registration Protocol) kann **im Modus „VLAN Tagging“** zur dynamischen Registrierung der VLANs am jeweiligen Nachbarn aktiviert werden. Der Schalter GVRP gibt die gewählte Benutzereinstellung wider oder erlaubt die Einstellung.

GVRP dient der dynamischen Bildung von VLANs über Switch-Grenzen hinweg. Ist GVRP auf „Disable“ gesetzt, so ist der Switch für GVRP-BPDUs (GVRP-Datenpakete) transparent.

Ist GVRP aktiv, sendet der Switch GVRP-BPDUs im Abstand von zehn Sekunden. Wird die VLAN-Zugehörigkeit **eines Ports** zu einem bestimmten VLAN verändert, dann bekommen benachbarte Switches die Änderung somit nach 10 Sekunden mitgeteilt,

Das Ausschalten des GVRP führt dazu, dass auch die benachbarten Switches die dynamisch gelernten Ports nach maximal zehn Sekunden entfernen. Bleiben GVRP Pakete aus, werden die erlernten Gruppenzugehörigkeiten nach ca. 20 Sekunden verworfen.

Ist auf einem Switch ein statisches VLAN eingerichtet, kann ein Port diesem VLAN über GVRP hinzugefügt werden. Der Port wird danach in der Current VLAN Table aufgelistet. Gespeichert werden aber nur die statisch angelegten Gruppenmitglieder.

8.4 Current VLANs

Die Webseite „Current VLANs“ bietet eine Übersicht über die aktuell eingerichteten VLANs. Zusätzlich ist der Tabelle das VLAN zu entnehmen, in dem das Management des Switches selber arbeitet (siehe auch „Webseite „IP Configuration““ auf Seite 4-14). In dieser Darstellung werden alle statischen und dynamischen VLANs aufgelistet. Dabei wird zwischen Gruppenmitglied mit Tag (T) und ohne Tag (U), sowie kein Gruppenmitglied (-) unterschieden (siehe möglich Stati auf Seite 8-5).

Current VLANs

VID	Status	Group	Membership
1	static / Management Vlan	Ports 1-8	U U U U U U U U
		Ports 9-16	U U U U U U U U
12	static	Ports 1-8	- T T - - - - -
		Ports 9-16	- - - - - - - -
24	static	Ports 1-8	- - - - - - - -
		Ports 9-16	- - - - T U - -

(T=Tagged, U=Untagged, -=Non Member)

*This table, indicates, out of which ports, each VLAN's data is to be sent, using configuration data entered manually (i.e. web page **Static VLANs**) or entered automatically from **GVRP**.*

Note: This web page will be refreshed in 23 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces')!

Bild 8-2 Webseite „Current VLANs“

Beim Erreichen der maximalen Anzahl an eingerichteten VLANs - statisch und/oder dynamisch - wird unterhalb der Legende zu den Mitgliedsstati der Text „The switch supports only 32 VLANs! Further VLANs will be refused!” eingeblendet.

Das VLAN 1 ist immer statisch eingerichtet und alle Ports sind als Untagged Mitglieder diesem hinzugefügt.

8.4.1 Static VLANs

Auf dieser Webseite legen Sie statische VLANs an. Sie können bis 31 VLANs neu anlegen (VLAN 2 bis VLAN 32), falls Sie weitere anlegen, wird ein entprechender Hinweis eingeblendet.

Das VLAN 1 ist immer statisch eingerichtet und alle Ports sind als Untagged Mitglieder diesem hinzugefügt. Die Netzwerk-basierten Management-Interfaces (WBM, Telnet und SNMP) sind im Auslieferungszustand mit aktiviertem VLAN-Modus „Tagging“ aus dem VLAN 1 heraus erreichbar. Das bedeutet: Um die Management-Interfaces zu erreichen, müssen Sie im Tagged-Modus entweder Datenverkehr ohne VLAN-Tag einrichten, der über Ports mit der VLAN-ID den Switch erreicht oder Sie müssen Datenverkehr mit VLAN-Tag der ID 1 nutzen.

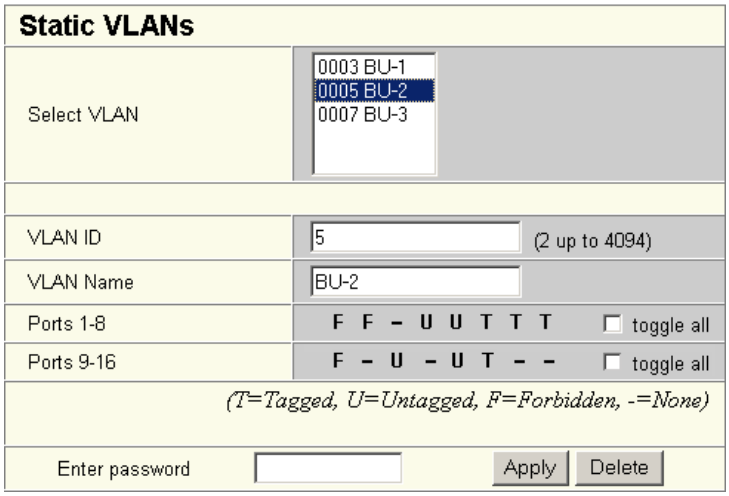


Bild 8-3 Menü „Static VLANs“

Auf dieser Webseite legen Sie statische VLANs an, indem Sie eine VLAN-ID und einen VLAN-Namen vergeben. Die Ports werden dann den einzelnen VLANs zugeordnet, indem Sie das jeweilige VLAN auswählen und in der Zeile „Ports 1-8“ usw. auf das Zeichen klicken, das den aktuellen Status des Ports anzeigt. Durch mehrfaches Klicken auf den Status werden die verschiedenen Möglichkeiten ausgewählt. Durch Klicken auf „toggle all“ verändern alle verfügbaren Ports in der jeweiligen Port-Gruppe ihren Status.

Mögliche Stati sind:

T = Tagged

Ports mit dem Status „Tagged“ gehören zu dem ausgewählten VLAN und Pakete werden an diesem Port mit VLAN-Tag versendet.

U = Untagged

Ports mit dem Status „Untagged“ gehören zu dem ausgewählten VLAN und Pakete werden an diesem Port ohne VLAN-Tag versendet. Ein „Untagged“ Port darf nicht Mitglied mehrerer VLANs sein - sonst besteht keine logische Trennung (außer VLAN1).

F = Forbidden

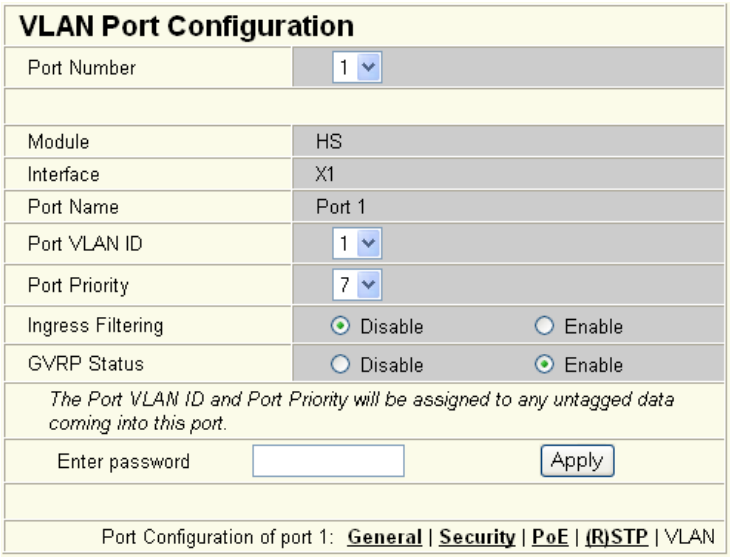
Ports mit dem Status „Forbidden“ gehören nicht zum ausgewählten VLAN und können nicht dynamisch über GVRP zu diesem VLAN hinzugefügt werden.

- **= None**

Ports mit dem Status „None“ sind nicht in das VLAN integriert.

8.4.2 VLAN Port Configuration

Auf dieser Webseite sind die portbezogenen VLAN-Einstellungen möglich.



Falls Sie „Ingress Filtering“ auf „Enable“ setzen, verwirft der Switch die an diesem Port ankommende Datenpakete, wenn der Port nicht zum VLAN mit der im Tag des Paketes enthaltenen VLAN ID als „Tagged“ oder „Untagged member“ gehört.

Port Priority

– Ein entsprechender Tag mit Angabe der Priorität wird in Pakete ohne Tag eingefügt.

Port VLAN ID

– Zuordnung von empfangenen, nicht getaggten Paketen zu einem VLAN. Die entsprechende VLAN-ID ist bei den Ports einzustellen, die „untagged“ Mitglied eines VLANs sind (siehe „Beispiel: Kommunikation zwischen Endgeräten über VLAN“ auf Seite 8-8).

Als Port VLAN ID können nur IDs von bereits angelegten VLANs eingestellt werden. Wird ein VLAN gelöscht, so fallen alle Port VLAN IDs, die auf dieses VLAN gesetzt sind, zurück auf die Default VLAN ID „1“.

8.4.3 VLAN Port Configuration Table

Diese Webseite bietet eine Übersicht über die wichtigsten VLAN-Einstellungen der Ports. Durch Klicken auf die jeweilige Portnummer wird die Webseite „VLAN Port Configuration“ geöffnet, auf der die Einstellungen geändert werden können.

Über diese Tabelle findet die Zuordnung von eingehenden Paketen zu den angelegten VLANs statt, wenn die Pakete den Port ohne VLAN-Tag erreichen.

Vlan Port Configuration Table

Module	Interface	Port	PVID	Prio	Ingress Filtering
HS	X1	1	1	7	disable
		2	1	0	disable
	X2	3	1	0	disable
		4	1	5	enable
	X3	5	1	0	disable
		6	1	0	disable
	X4	7	1	0	disable
		8	1	0	disable

This table indicates what Port VLAN ID and Priority will be assigned to any untagged data coming in each port.

Enter password [ ] Apply

Bild 8-4 Menü „Vlan Port Configuration Table“

8.5 Einrichten von statischen VLANs

Security-Empfehlung: Anstatt VLAN 1 für das Management zu nutzen, ist es empfehlenswert, für das Management ein eigenes neues VLAN anzulegen. Stellen Sie dabei sicher, dass der Administrator Zugriff auf dieses VLAN hat.

Warnhinweise bei der Einrichtung/Konfiguration von VLANs weisen auf Konfigurationsfehler hin:

– Ein „untagged“ Port ist Mitglied **mehrerer** VLANs.
– Die Port-Mitgliedschaft (untagged) und PVID stimmen **nicht** überein.

Um ein VLAN einzurichten, müssen die beteiligten Switches entsprechend konfiguriert werden. Im folgenden Beispiel ist das Ziel, einen Datenverkehr im VLAN 5 zwischen den Endgeräten A und B zu ermöglichen.

Dabei ist die Art der Endgeräte zu berücksichtigen: VLAN-fähig (verarbeitet Tags) oder nicht VLAN-fähig (verarbeitet keine Tags). Im Beispiel sind beide Endgeräte-Typen berücksichtigt.

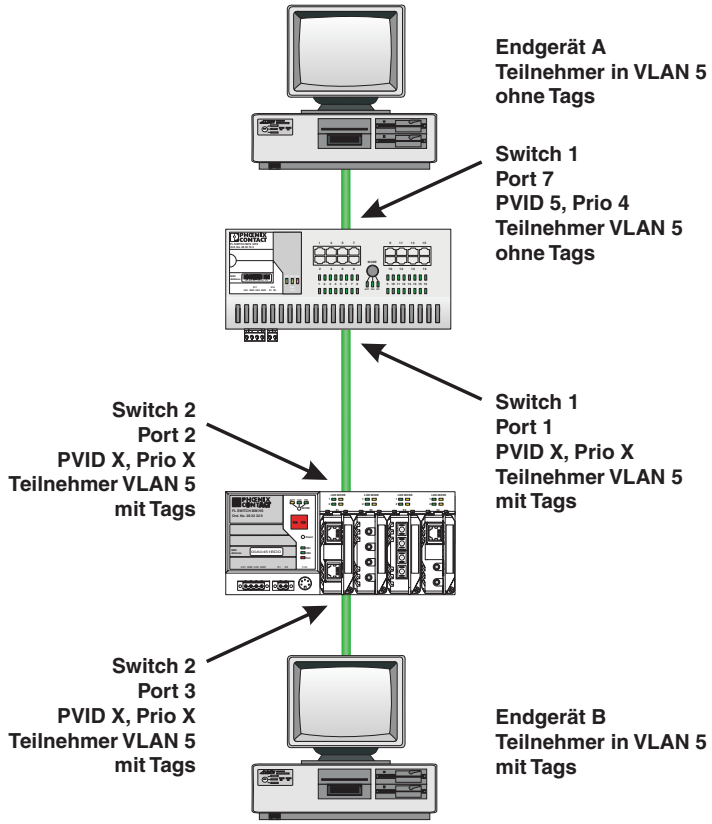


Bild 8-5 Beispiel: Kommunikation zwischen Endgeräten über VLAN

Konfiguration der Switches

1. Beide Switches in den Modus „VLAN Tagging“ setzen, speichern und Geräte neu starten.
2. Auf Switch 1 VLAN 5 einrichten und den Port 7 als „Untagged“ Mitglied und den Port 1 als „Tagged“ Mitglied angeben.
3. Für den Port 7 am Switch 1 die Port VLAN ID auf 5 und die Port Priorität auf beliebig setzen.
4. Auf Switch 2 Port 2 und Port 3 als „Tagged“ Member im VLAN 5 einrichten.

Die beiden Endgeräte kommunizieren nun über den im Beispiel dargestellten Netzwerkpfad, ohne dass andere Ports der Switches, z.B. Broadcast-Pakete der beiden Endgeräte weiterleiten.

Befinden sich zwischen dem Switch 1 und dem Switch 2 weitere Infrastruktur-Komponenten gibt es zwei Möglichkeiten, die Kommunikation zwischen den Endgeräten sicher zu stellen:

1 Die Infrastruktur wird ebenfalls im Modus „VLAN Tagging“ betrieben und das VLAN 5 ist jeweils auf den Geräten eingerichtet. Ergebnis: hoher Konfigurations- und Pflege-Aufwand.

2 Das GVRP wird im Modus „VLAN Tagging“ auf allen Infrastruktur-Komponenten aktiviert und die Informationen über die eingerichteten VLANs werden jeweils von Switch 1 und Switch 2 im Netzwerk verbreitet. Ergebnis: der bidirektionale Datenaustausch zwischen Endgerät A und B wird sichergestellt.

8.5.1 Dynamische Konfiguration

Zwischen Infrastruktur-Komponenten kann auf die dynamische VLAN-Konfiguration durch das GVRP gesetzt werden. Dabei sendet jeder Switch mit statisch oder dynamisch eingerichteten VLANs die Informationen über die VLAN-IDs ins Netzwerk und die benachbarten Switches mit aktiviertem GVRP legen daraufhin dieselben VLANs an und fügen die Empfänger-Ports der GVRP-BPDUs als „Tagged“ Port ein. Ein BPDU-Empfänger verteilt dann selbst auch wieder an allen Ports eigene BPDUs über das dynamische erlernte VLAN.

Konfiguration der Switches

1 Alle Switches müssen in den Modus „VLAN Tagging“ gesetzt werden. Nach dem Speichern der Konfiguration ist ein Neustart erforderlich.

2 Auf allen Switches ist GVRP zu aktivieren.

Da Endgeräte im Regelfall keine VLAN-Tags unterstützen, sind an den Endgeräte-Ports der Infrastruktur Port-spezifische Einstellungen vorzunehmen. Der Switch fügt dann in alle an dem jeweiligen Port empfangenen Datenpakete die entsprechenden Tags ein. Soll ein Datenpaket vom Endgeräte-Port an das Endgerät geschickt werden, entfernt der Switch zuvor den VLAN-Tag.

8.6 VLAN & (R)STP

Bei gleichzeitiger Nutzung von (R)STP und VLAN ist folgendes zu beachten:

– (R)STP orientiert sich **nicht** an den VLANs

– (R)STP baut eine schleifenfreie Topologie in Form einer Baumstruktur auf

Bei der statischen VLAN-Konfiguration müssen alle möglichen redundanten Datenpfade bei der Konfiguration berücksichtigt werden. Alle möglichen Backbone-Ports des Netzwerkes (also nicht die Endgeräte-Ports) müssen in allen verfügbaren VLANs als „tagged“ hinzugefügt werden. Dadurch wird sichergestellt, dass bei jeder möglichen Baumstruktur, die durch (R)STP erzeugt werden kann, jedes VLAN durch jeden Switch erreicht werden kann.

Eine beispielhafte Konfiguration ist in nachfolgender Grafik dargestellt:

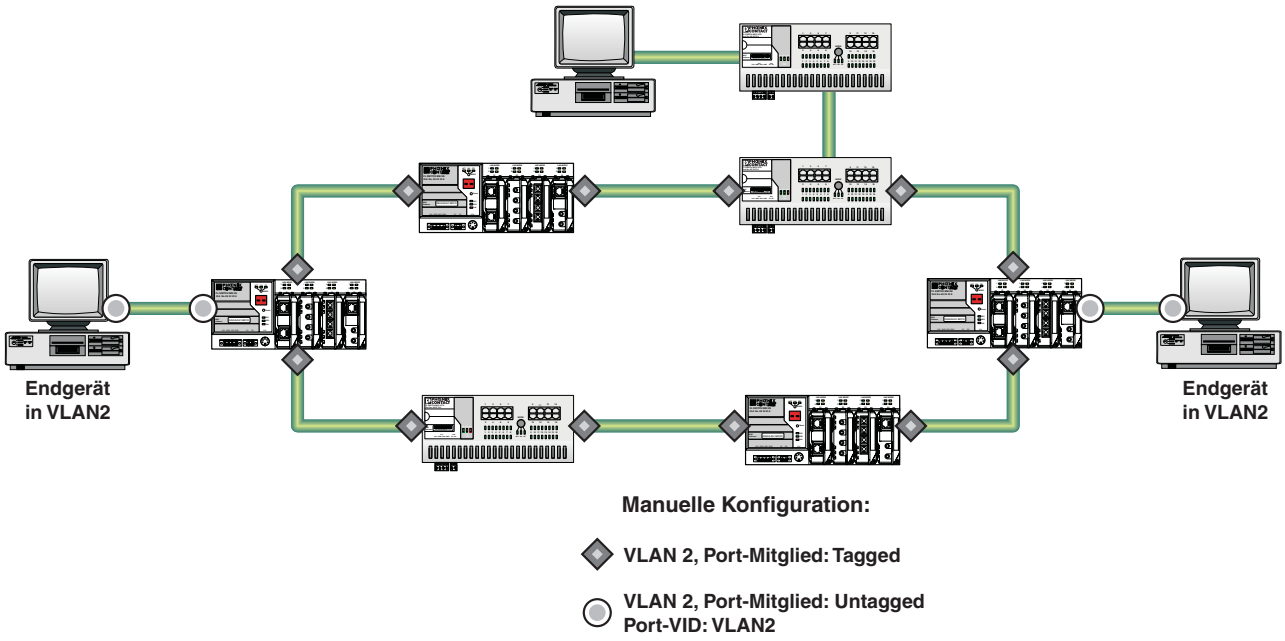


Bild 8-6 Beispielhafte Konfiguration bei VLAN & (R)STP

9 Betrieb als PROFINET-Device

Der Switch wird als PROFINET-Device ab der PC WorX-Version 5.00.26 unterstützt. Innerhalb einer PROFINET-Applikation übernimmt dann der PROFINET IO-Controller die Inbetriebnahme des Switches. Dazu gehört die Vergabe der IP-Parameter, der Vergleich der Soll-/Ist-Konfiguration und die Archivierung der vom Switch versendeten Alarme. Im Falle eines Gerätetausches erkennt die Steuerung das Austauschgerät und nimmt dieses selbstständig in Betrieb. Für das Steuerungsprogramm stellt der Switch als PROFINET IO-Device die Link-Stati als Prozessdatum zur Verfügung.

9.1 Vorbereitung des Switches für die PROFINET-Betriebsart

Der Switch arbeitet im Auslieferungszustand in der Betriebsart „Normal“ und muss einmalig in die Betriebsart „Profinet“ gesetzt werden.

Umschaltung in die Betriebsart „Profinet“

Die Umschaltung kann über zwei Mechanismen erfolgen:

– Nach Inbetriebnahme und Vergabe einer IP-Adresse kann die Betriebsart im WBM auf der entsprechenden Seite (siehe Kapitel „Menü „Operating Mode““ auf Seite 4-20) geändert werden oder
– durch Konfiguration über die serielle Schnittstelle (siehe Kapitel „Management über lokale V.24-Kommunikationsschnittstelle“ auf Seite 4-121).

Bei der Aktivierung der Betriebsart „Profinet“ werden folgende Voreinstellungen für den Betrieb vorgenommen:

– Das Link Layer Discovery Protocol (LLDP) wird mit folgenden Konfigurationsvorgaben für PROFINET-Komponenten eingeschaltet
  - Message Transmit Interval: 5 s
  - Message Transmit Hold Multiplier: 2
  - TLV Port ID mit Subtype Locally Assigned im Format: port-xyz
  - TLV Chassis ID mit Subtype Locally Assigned überträgt den Stations-Namen
– Das Discovery and Configuration Protocol (DCP) wird als Mechanismus zur Vergabe der IP-Parameter aktiviert.
– Der Stations-Name (System Name) wird gelöscht, wenn der Wert für das Objekt „System Name“ den Gerätetyp (Auslieferungszustand) beinhaltet.
– Das MRP-Protokoll ist nicht aktiviert.

Zusätzlich wird beim Wechsel in die Betriebsart „Profinet“ die Konfiguration automatisch gespeichert und ein Neustart des Gerätes durchgeführt.

Der Switch startet danach erstmalig in der Betriebsart „Profinet“ und wartet auf die Taufe sowie auf Zuweisung einer PROFINET-IP-Adresse. Zu diesem Zeitpunkt ist der Switch über das LLDP bereits mit dem Default-Namen „FL SWITCH MM HS“ und der IP-Adresse „0.0.0.0“ im Netzwerk sichtbar.

Das Warten auf eine gültige IP-Konfiguration über DCP wird vom Switch durch die Anzeige „dP“ auf dem Display und durch das Blicken der zu diesem Zeitpunkt aktiven Mode-LED signalisiert.

Über andere Netzwerkdienste, wie Ping, ist der Switch zu diesem Zeitpunkt nicht erreichbar.

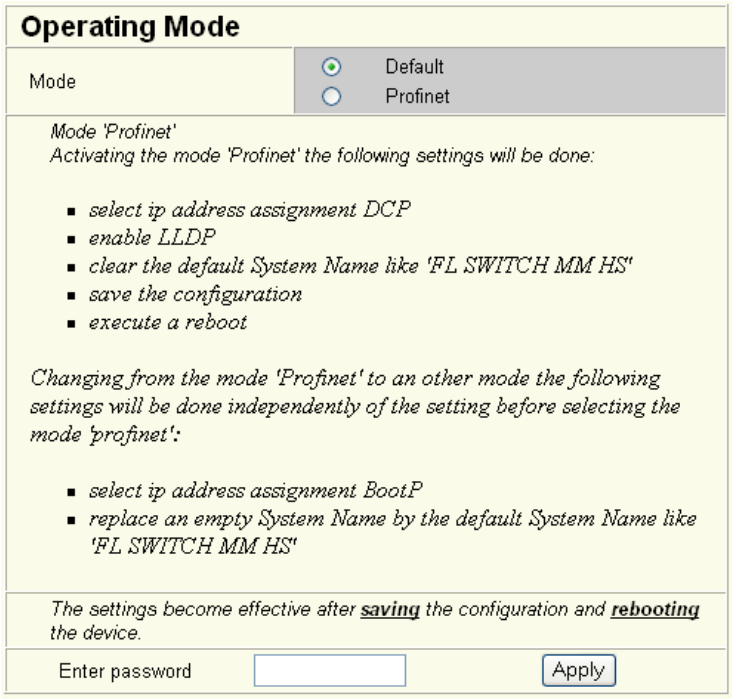

Operating Mode
Mode
Default
Profinet
Mode 'Profinet'
Activating the mode 'Profinet' the following settings will be done:
select ip address assignment DCP
enable LLDP
clear the default System Name like 'FL SWITCH MM HS'
save the configuration
execute a reboot
Changing from the mode 'Profinet' to an other mode the following settings will be done independently of the setting before selecting the mode 'profinet':
select ip address assignment BootP
replace an empty System Name by the default System Name like 'FL SWITCH MM HS'
The settings become effective after saving the configuration and rebooting the device.
Enter password
Apply

Bild 9-1 Webseite „Operating Mode“

Umschaltung in die Betriebsart „Normal“

Wird der Switch aus der Betriebsart „Profinet“ zurück in die Betriebsart „Normal“ gesetzt, werden folgende Einstellungen vorgenommen:

– LLDP bleibt mit den Werten des Auslieferungszustandes weiterhin aktiv.
– Die Vergabe der IP-Adresse wird auf BootP gesetzt.
– Der Stations-Name des Switches wird nicht verändert. Falls kein Stations-Name festgelegt wurde, wird der Gerätetyp eingetragen.

Es wird empfohlen, nach einem Wechsel der Betriebsart die neue Konfiguration zu speichern. Beachten Sie, dass einige Konfigurationsänderungen erst nach einem Neustart wirksam werden.

9.2 Switch als PROFINET IO-Device

9.2.1 Projektierung im Engineering-Werkzeug

9.2.1.1 Busaufbau vorgeben

Der Switch kann als PROFINET IO-Device betrieben werden, wenn er im Engineering-Werkzeug unterhalb einer Steuerung in den Busaufbau integriert wird. Für die Integration steht eine GSD- und eine FDCML-Datei zum Download unter www.download.phoenixcontact.de zur Verfügung.

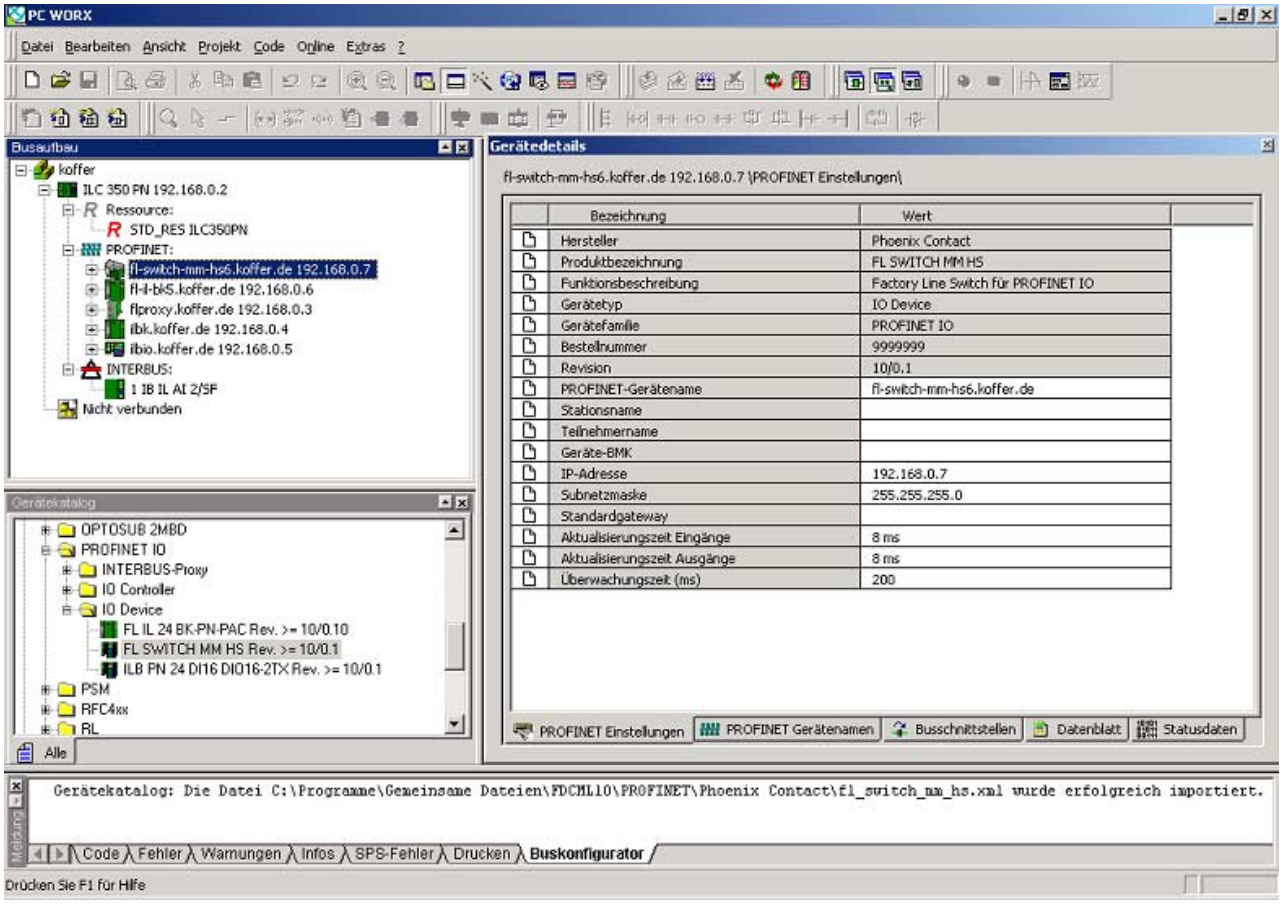


Bild 9-2 Der Switch im Busaufbau unter PC WorX

Falls der Switch nicht im Gerätekatalog aufgeführt ist, muss die von Phoenix Contact zur Verfügung gestellte Gerätebeschreibung importiert werden. Sie finden die aktuelle Gerätebeschreibung im Internet unter www.download.phoenixcontact.de.

Wenn die Gerätebeschreibung im Gerätekatalog zur Verfügung steht, gibt es folgende Möglichkeiten den Busaufbau zu projektieren:

– Manuell - die Komponenten werden per Drag & Drop aus dem Gerätekatalog in den Busaufbau übernommen.
– Automatisch - über die Funktion „Profinet einlesen“ werden die Geräte erfasst, so dass sie im Netzwerk über DCP (Discovery and Configuration Protocol) erreichbar sind. Dazu müssen die Geräte mit Spannung versorgt sein und die Betriebsart muss „Profinet“ sein.

Interface-Module und Busaufbau

– Keine Interface-Module projektiert -> nur IP-Adressvergabe durch die Steuerung
– Alle Interface-Module korrekt projektiert -> IP-Adressvergabe durch die Steuerung, Übertragung von Prozessdaten und Alarmen von projektierten Slots

– Mindestens ein Interface-Modul falsch projektiert -> Nach dem Start zeigt der MMS im Display „Cd“ (Configuration difference).

Stecken Sie bei der Display-Anzeige „Cd“ die richtigen Interface-Module und starten Sie anschließend den Switch neu.

Zur Laufzeit des Systems wird die Soll-/Ist-Konfiguration nicht mehr überwacht.

9.2.2 Switch als PROFINET IO-Device projektieren

Wenn alle Switches in den Busaufbau aufgenommen sind, müssen folgende Einstellungen für die einzelnen Switches über den Reiter „Detail View“ (Gerätedetails) vorgenommen werden:

– Der PROFINET-Gerätename muss geprüft und gegebenenfalls geändert werden.
– Die IP-Adresse und die Subnetzmaske müssen geprüft und gegebenenfalls geändert werden.
– Die Aktualisierungszeit für Eingänge sollte auf den Wert **„512 ms“** (Default) eingestellt sein.
– Die Aktualisierungszeit für Ausgänge sollte auf den Wert **„512 ms“** (Default) eingestellt sein.
– Die Überwachungszeit sollte auf den Wert **„2000 ms**“ (Default) eingestellt sein.
– Die Interface-Module müssen aus dem Modulkatalog ausgewählt und zur Station hinzugefügt werden.

Gerätedetails

FL SWITCH MM HS pn-mms61 172.16.27.61 \PROFINET Einstellungen\

Bezeichnung	Wert	
Hersteller	Phoenix Contact	
Produktbezeichnung	FL SWITCH MM HS	
Funktionsbeschreibung	Modularer managbarer Switch als Profinet IO D...	
Gerätetyp	Switch	
Gerätefamilie	FL	
Bestellnummer	2832328	**Durch den Anwender eingestellt:**
Revision	00 / 4.00	
DNS/PROFINET-Gerätename	fl-switch-mm-hs6.koffer.de	← **Stationsname**
Stationsname		
Teilnehmername		
Geräte-BMK		
IP-Adresse	172.16.27.61	← **IP-Adresse**
Subnetzmaske	255.255.0.0	← **Subnetzmaske**
Standardgateway		
Aktualisierungszeit Eingänge	512 ms	
Aktualisierungszeit Ausgänge	512 ms	
Überwachungszeit (ms)	2000	← **Empfohlener Wert**
Betrieb bei Konfigurationsunterschieden	nein	
Oberster Knoten in Ethernet-Topologie	nein	
Verbindungszustand protokollieren	ja	

687407055

Bild 9-3 Gerätedetails mit geänderten Einstellungen

Danach können im Steuerungsprogramm die PROFINET-Variablen angelegt und verwendet werden.

Der Switch stellt neben der Standard-Variablen „PNIO_DATA_STATE“ für jeden Port den Link-Status als Prozessdaten-Byte zur Verfügung. Erklärt das Bit „PNIO_DATA_VALID“ der Variablen „PNIO_DATA-STATE“ die Prozessdaten des Switches als gültig, dann kann das Prozessdatum eines Ports die folgenden Werte annehmen:

– Wert = 1 - aktiver Link
– Wert = 2 - kein aktiver Link
– Wert = 3 - Link vorhanden, aber die Gegenstelle kann den Link nicht aufbauen (nur bei FX-Ports - Far End Default Detection)

Auf Prozessdaten kann nur zugegriffen werden, wenn die parametrierte Soll-Konfiguration beim Geräteanlauf mit der Ist-Konfiguration übereingestimmt hat.

Das „Status“- und das „Control“-Wort des Management Agent werden nicht benutzt.

9.2.3 PROFINET-Blink-Funktion

Wenn der Switch im PROFINET-Modus vom Engineering zum Blinken aufgefordert wird, blinkt das Display im Wechsel mit „00“ und der zuvor aktuellen Anzeige.

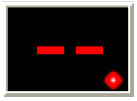
9.2.4 Gerätetaufe

Zur Inbetriebnahme eines Switches in der Betriebsart „Profinet“ muss einmalig jeder Switch getauft werden - jedem PROFINET-Gerät wird ein eindeutiger Gerätename zugewiesen. Dazu wird über das Engineering-Tool eine Gerätesuche (Funktion „PROFINET einlesen“ bei PC WorX) durchgeführt, bei der alle erreichbaren Geräte im Netzwerk aufgelistet werden. Nach einer Identifizierung der unbekannten Teilnehmer über die angegebene MAC-Adresse oder die Funktion „Blinken“ wird der im Engineering projektierte Gerätename dauerhaft auf dem Switch mit der Funktion „Namen vergeben“ hinterlegt.

Die Vergabe des Gerätenamens/Taufe kann auch vor dem Wechsel in die Betriebsart „Profinet“ über das WBM durchgeführt werden.

9.2.5 Betrieb im PROFINET-Umfeld

Ein Switch, der bereits getauft ist, startet in der Betriebsart „Profinet“ ohne IP-Adresse und wartet auf die Zuweisung einer IP-Konfiguration (Anzeige im Display „dP“ und dem Blinken der zu dem Zeitpunkt aktiven Mode-LED). Nachdem das Projekt übersetzt und auf die Steuerung herunter geladen wurde, übernimmt die Steuerung die Inbetriebnahme und die Konfiguration. Sobald erfolgreich eine Kommunikationsbeziehung zwischen Switch und Steuerung hergestellt ist, startet der Switch seine Management-Interfaces. Durch einen Eintrag in die Ereignis-Tabelle und durch einen zusätzlichen Punkt rechts unten im Display signalisiert der Switch den korrekten Aufbau der PROFINET-Verbindung.



Wenn der MMS eine PROFINET-Verbindung aufgebaut hat, zeigt das Display unten rechts einen Punkt.

9.3 Alarme bei PROFINET

Der MMS ist in der Lage, folgende Alarme zu versenden:

– Fehlen der redundanten Spannungsversorgung (Alarm vom Management Agent)
– MRP-Manager registriert eine Ring-Unterbrechung (Alarm vom Management Agent)
– Entfernen eines Interface-Moduls (Alarm vom jeweiligen Slot)
– Linküberwachung (Alarm vom Slot für jeweiligen Channel/Port)
– POF-SCRJ Diagnostic Alarm für Erreichen und Überschreiten der Warnschwelle (Alarm vom Slot für jeweiligen Channel/Port)

Die Alarme sind alle bei Gerätestart deaktiviert.

9.3.1 Alarme im WBM

In der Betriebsart „Profinet“ wird in der Navigationsbar unter „Switch Station/ Diagnostics“ die Webseite „Profinet Alarms“ angeboten. Dort ist die Möglichkeit gegeben alle vom IO Device unterstützten Alarme zu aktivieren. Die PROFINET-Alarme werden von den IO Devices an die Steuerung geschickt. Von dort können Sie mit dem Tool „DIAG+“ (Version 2.0 ist im Service Pack 1 zu PC WorX 5.00.26 enthalten) aus dem Diagnosearchiv ausgelesen werden.

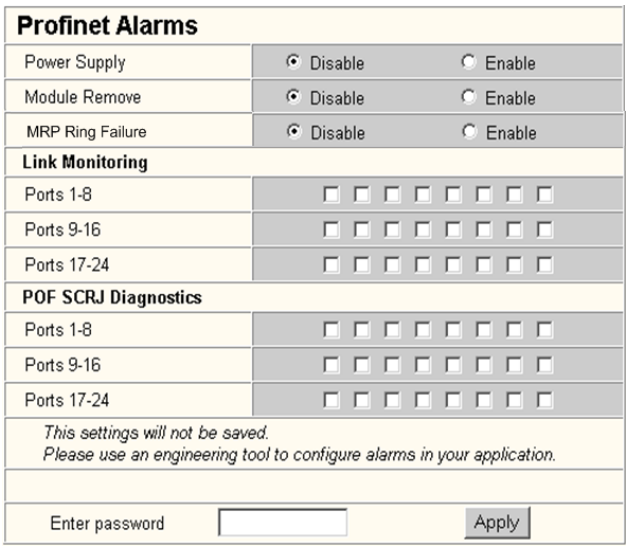


Bild 9-4 PROFINET-Alarme im WBM

Die Einstellung der Profinet Alarme kann mit der Konfiguration gespeichert werden. Der Controller kann eine abweichende Alarm-Konfiguration an den Switch übertragen und damit die Konfigurationseinstellungen überschreiben.

9.4 Prozessdatenkommunikation

9.4.1 Control Word

Das Control Word ist ein spezielles Prozessdatum, um Einstellungen vorzunehmen, die nicht über ein übliches Prozessdatum ausgeführt werden soll.

Dazu kann das Control Word des Management Agents mit einem Kommando bestehend aus zwei Byte beschrieben werden, woraufhin das Device mit dem selben Kommando im Status Word antwortet. Byte 0 gibt die Aktion und den neuen Status an; Byte 1 gibt die Port-Nummer an. Soll ein Kommando für alle Ports gelten, dann kann statt der Portnummer der Wert 0xFF gesendet werden. Ein Kommando sollte jeweils nur einmal, auf keinen Fall aber im Zyklus der Prozessdaten-Kommunikation, gesendet werden.

Tabelle 9-1 Belegung des Control Words

Aktion	Status	Byte 0	Byte 1
Link-Überwachung	Ein	0x01	Port oder 0xFF
	Aus	0x02	Port oder 0xFF
POF SCRJ Diagnose	Ein	0x03	Port oder 0xFF
	Aus	0x04	Port oder 0xFF
Spannungsversorgung	Ein	0x05	0x00
	Aus	0x06	0x00
Interface entfernt	Ein	0x07	0x00
	Aus	0x08	0x00
MRP Ring Failure	Ein	0x09	0x00
	Aus	0x0a	0x00
Link Enable Status	Ein	0x20	Port
	Aus	0x21	Port

9.4.1.1 Weitere Prozessdaten

Der MMS ist in der Lage folgende Prozessdaten zu senden:

– Zusammenfassung der Link-Stati aller Ports (drei Byte) - jeder Port entspricht einem Bit (0 - Link Down; 1 - Link Up)

Byte	1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3
Bit	7	6	5	4	3	2	1	0
Port	8/16/24	7/15/23	6/14/22	5/13/21	4/12/20	3/11/19	2/10/18	1/9/17

– Die Slots senden Link-Informationen für jeden Port. Darin sind enthalten
  - Link-Status: (0 - Link Down; 1 - Link Up)
  - Status Far-End-Fault: (0 - kein Fehler; 1 - Fehler)
  - Port Enable Status: (0 - Enabled; 1 - Disabled)
  - Linkmode: (0 - Forwarding; 1 - Blocking)

Bit	7	6	5	4	3	2	1	0
Bedeutung	Linkmode					Port Enable	Far-End-Fault	Linkstatus

10 LLDP - Link Layer Discovery Protocol

10.1 Grundlagen

LLDP

Der Switch unterstützt LLDP nach IEEE 802.1ab und ermöglicht so eine Topologie-Erkennung von Geräten, die ebenfalls LLDP aktiviert haben.

Vorteile durch die Verwendung von LLDP:

– Verbesserte Fehlerort-Erkennung.
– Verbesserter Gerätetausch.
– Effizientere Netzwerk-Projektierung.

Folgende Informationen werden von Nachbarn empfangen oder an Nachbarn versendet, sofern LLDP aktiviert ist:

– Das Gerät versendet die eigenen Management- und Verbindungsinformationen an benachbarte Geräte.
– Das Gerät empfängt Management- und Verbindungsinformationen von benachbarten Geräten.

Anzeige der LLDP-Informationen

Die gesammelten Informationen werden im WBM in Form einer Tabelle aufbereitet. Die Tabelle enthält die beiden Port-Nummern, über die die beiden Geräte miteinander verbunden sind, sowie die IP-Adresse und den Device-Name der Nachbargeräte sowie den Gerätetyp.

LLDP General

Das Link Layer Discovery Protocol (LLDP) nach 802.1ab dient Netzwerkteilnehmern dazu, die eigenen Nachbarschaftsbeziehungen zu erlernen und zu pflegen.

Funktion

Eine Netzwerkinfrastruktur-Komponente sendet zur Verbreitung von Topologie-Informationen im zeitlichen Abstand vom „Message Transmit Interval“ an jedem Port eine Port-bezogene BPDU (Bridge Protocol Data Unit) aus, die die eigenen Geräte-Informationen enthält. Die an dem jeweiligen Port angeschlossene Gegenstelle erlernt durch diese BPDUs Port-bezogen ihre jeweiligen Nachbarn.

Die durch die BPDUs erlernten Informationen werden für eine definierte Zeitspanne, dem TTL-Wert (TTL - Time To Live), gespeichert. Durch den erneuten Empfang der gleichen BPDUs wird der TTL-Wert wieder erhöht und die Information bleibt gespeichert. Läuft die TTL ab, wird die Nachbarschaftsinformation gelöscht.

Ein MMS verwaltet maximal 50 Nachbarschaftsinformationen, darüber hinaus gehende Informationen werden ignoriert.

Falls an einem Switch-Port mehrere Nachbarn angezeigt werden, ist **zwischen** diesem Switch und den angezeigten Nachbarn mindestens **ein weiterer** Switch/Hub installiert, der LLDP nicht unterstützt oder nicht aktiviert hat.

Tabelle 10-1 Ereignistabelle bei LLDP

Ereignis	Aktion des eigenen LLDP-Agenten	Reaktion des LLDP-Agenten des Nachbarns
LLDP-Agent aktivieren oder Gerätestart	LLDP-BPDUs an allen Ports versenden	Absender in die Liste der Nachbarn aufnehmen
LLDP-Agent deaktivieren oder Software-Reset	LLDP-BPDUs mit dem TTL-Wert von 0 Sekunden an allen Ports versenden	Absender aus der Liste der Nachbarn löschen
Link-Up	Port-bezogene LLDP-BPDUs senden	Absender in die Liste der Nachbarn aufnehmen
Link-Down	Alle Nachbarn dieses Ports löschen	-
Timer (Message Transmit Interval)	Zyklisches Senden der BPDUs an allen Ports	Informationen aktualisieren
Aging (Time To Live)	Nachbarschaftsinformation löschen	-
Empfang einer BPDU von einem neuen Nachbarn	Nachbarschaftsliste erweitern und mit Port-bezogener BPDU antworten	Absender in die Liste der Nachbarn aufnehmen

Link Layer Discovery Protocol

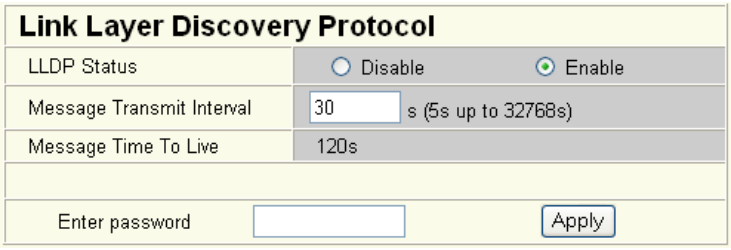


Bild 10-1 Webseite „Link Layer Discovery Protocol“

Die „Message Time To Live“ wird durch Multiplikation des „Message Transmit Interval“ mit dem „Message Transmit Hold Multiplier“ ermittelt. Der „Message Transmit Hold Multiplier“ ist nur über SNMP veränderbar. Der Default-Wert ist vier.

LLDP Topology

LLDP Topology

Local	Neighbors			
Port	Type	Address	Device	Port
1		192.168.0.45	FL SWITCH MM HS	7
12		192.168.0.3	fl-il-bk2.quicks...	port-001
11		192.168.0.5	fl-pn-ibs4.quick...	port-001

Note: This web page will be refreshed in 26 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces)!

Bild 10-2 Webseite „LLDP Topology“

Für bekannte Nachbarn wird eine Tabelle angelegt, die folgende fünf Spalten enthält:

– Local Port
  Enthält die Nummer des Ports des lokalen Switches, über den ein Nachbar an diesen Switch angeschlossen ist. Die Port-Nummer ist gleichzeitig ein Link auf die lokale Webseite „Port Configuration“
– Type
  Hier wird ein Symbol angezeigt, das dem Gerätetyp des Nachbarn entspricht. Bei Geräten anderer Hersteller wird hier allgemein „Ethernet Device“ angezeigt.
– Address
  Zeigt die Management-IP-Adresse des Nachbarn.
– Device
  Zeigt den System-Namen des Nachbarn an.
– Zeigt die Port-Nummer des Nachbar-Switches an, über den der Nachbar mit dem lokalen Switch verbunden ist. Wenn der Nachbar als Switch von Phoenix Contact erkannt wird, ist die Port-Nummer als Link zur Webseite „Port Configuration“ des Nachbarn ausgeführt.

10.2 Darstellung der Topologie in einem Engineering-Tool

Die LLDP-Informationen können so oder ähnlich in Engineering-Tools dargestellt werden.

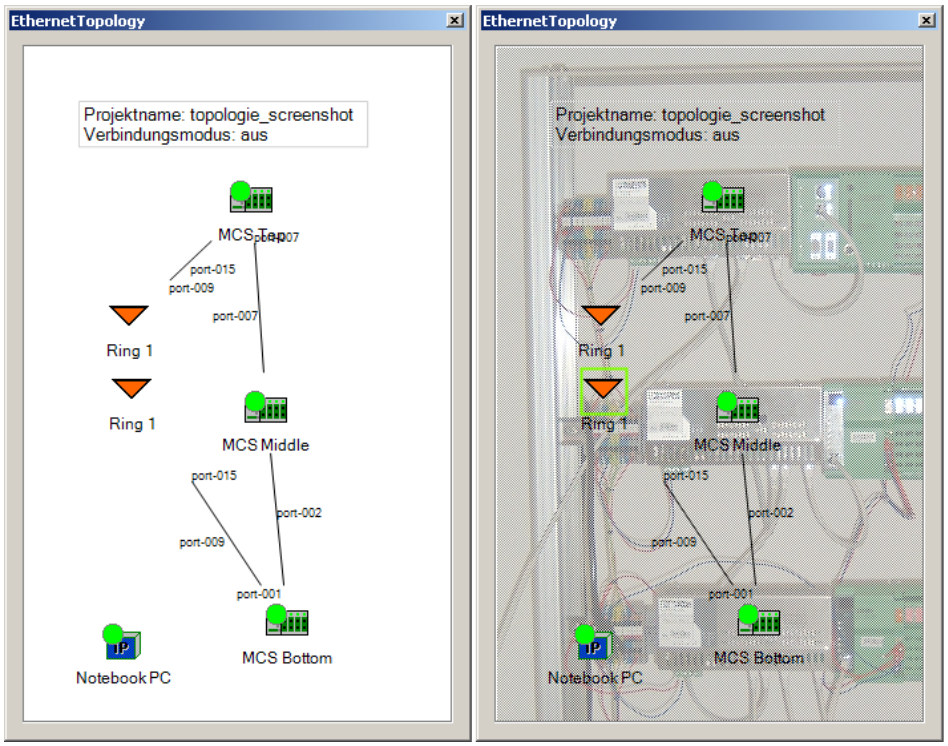


Bild 10-3 Topologie-Darstellung

11 DHCP Relay Agent

Der MMS ist in der Lage, als DHCP Relay Agent zu agieren. Die Funktion eines DHCP Relay Agenten wird für die sogenannte DHCP Option 82 benötigt. Die DHCP Option 82 dient dem DHCP-Server bei der Adresszuweisung zur Identifizierung des anfragenden Endgerätes über den zugehörigen physikalischen Switch-Port. Die DHCP Option 82 ermöglicht es dadurch, im Fall eines Gerätetausches dem Ersatzgerät aufgrund der physikalischen Position im Netzwerk die selbe IP-Adresse wie dem ausgetauschten Teilnehmer zu vergeben. Das vom Endgerät ursprünglich ausgesendete DHCP-Paket (Broadcast) erreicht ebenfalls den DHCP-Server, wenn dieser sich im gleichen Subnetz befindet. Der DHCP-Server sollte so eingestellt sein, dass er dieses Paket ignoriert.

Ablauf:

Immer wenn der MMS einen von einem Endgerät abgesendeten DHCP-Discover/Request empfängt, ergänzt der MMS das „DHCP Option 82“-Feld und leitet das Datenpaket zielgerichtet an den DHCP-Server weiter. Der gewünschte DHCP-Server ist im WBM auf der Seite „Relay Agent“ zu konfigurieren.

Der DHCP-Server kann unter Zuhilfenahme der Option-82-Informationen eine Antwort generieren und diese dem Relay Agenten zusenden.

Aus der Antwort des DHCP-Servers entfernt der Switch jetzt die DHCP Option 82-Daten und leitet die DHCP-Antwort an das Endgerät weiter, das den Request ausgelöst hat.

Informationen im DHCP Option 82-Feld:

Der MMS ergänzt im DHCP Option 82-Feld die VLAN-ID des VLANs, dem das Endgerät zugeordnet ist und den Switch-Port, an den das Endgerät angeschlossen ist. Außerdem trägt der MMS seine eigene DHCP Option 82 Remote-ID in das Feld ein. Die DHCP Option 82 Remote-ID kann durch den Anwender konfiguriert werden und enthält entweder die IP- oder die MAC-Adresse des MMS.

11.1 Aktivierung des DHCP Relay Agents

Schalten Sie die Webseite über „General Configuration/User Interfaces“ frei. Aktivieren Sie den Agent mit „Enable“ geben Sie mindestens die IP-Adresse des Servers an.

Das Management des MMS startet den Relay Agenten nicht, solange der Switch selbst als DHCP-Client arbeitet.

11.1.0.1 Relay Agent portbezogen abschaltbar

Ab der Firmware-Version 4.50 ist die Funktion DHCP Relay Agent portbezogen abschaltbar. Von den deaktivierten Ports werden keine DHCP-Option 82-Pakete gesendet.

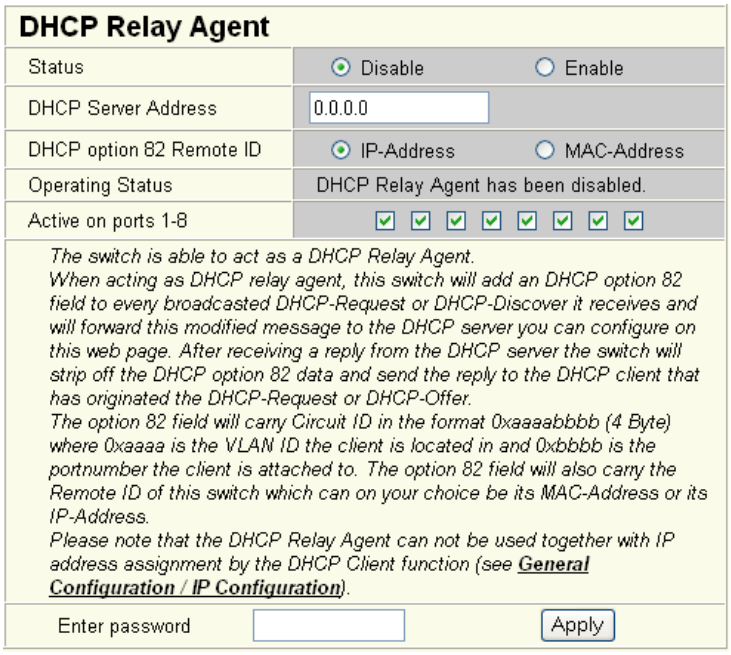

DHCP Relay Agent
Status
Disable
Enable
DHCP Server Address
0.0.0.0
DHCP option 82 Remote ID
IP-Address
MAC-Address
Operating Status
DHCP Relay Agent has been disabled.
Active on ports 1-8
The switch is able to act as a DHCP Relay Agent.
When acting as DHCP relay agent, this switch will add an DHCP option 82 field to every broadcasted DHCP-Request or DHCP-Discover it receives and will forward this modified message to the DHCP server you can configure on this web page. After receiving a reply from the DHCP server the switch will strip off the DHCP option 82 data and send the reply to the DHCP client that has originated the DHCP-Request or DHCP-Offer.
The option 82 field will carry Circuit ID in the format 0xaaaabbbb (4 Byte) where 0xaaaa is the VLAN ID the client is located in and 0xbbbb is the portnumber the client is attached to. The option 82 field will also carry the Remote ID of this switch which can on your choice be its MAC-Address or its IP-Address.
Please note that the DHCP Relay Agent can not be used together with IP address assignment by the DHCP Client function (see General Configuration / IP Configuration).
Enter password
Apply

Bild 11-1 Webseite „Relay Agent“

Die Funktion „DHCP Relay Agent“ und die IP-Adressvergabe per DHCP können nicht gleichzeitig aktiviert werden.

12 Technische Daten und Bestelldaten

12.1 Technische Daten

Allgemeine Daten	
Funktion	Modularer managed Ethernet/Fast Ethernet-Switch; normkonform nach IEEE 802.3
Switch-Prinzip	Store and Forward
Adresstabelle	8000 MAC-Adressen
SNMP	Version 1 und 2c
Transmission Capacity pro Port 64 Byte Paketgröße, Halbduplex	bei 10 MBit/s: 14880 pps (packets per second) bei 100 MBit/s: 148800 pps
Unterstützte MIBs	MIB II, RMON-MIB, Bridge-MIB, If-MIB, Etherlike-MIB und die privaten SNMP-Objekte von Phoenix Contact
Gehäusemaße (Breite x Höhe x Tiefe) in mm	
Kopfstation	214 x 95 x 107 (Tiefe ab Oberkante Hutschiene)
Kopfstation mit einem Erweiterungsmodul	341 x 95 x 107 (Tiefe ab Oberkante Hutschiene)
Kopfstation mit zwei Erweiterungsmodulen	468 x 95 x 107 (Tiefe ab Oberkante Hutschiene)
Zulässige Betriebstemperatur	0 °C bis 55 °C
Zulässige Lagertemperatur	-20 °C bis +70 °C
Schutzart	IP20, DIN 40050, IEC 60529
Schutzklasse nach EN 61131-2, IEC 61131-2	3
Laserschutz - LWL-Interface-Module	Klasse 1 nach EN 60825-1
Luftfeuchtigkeit	
Betrieb	10 % bis 95 %, nicht kondensierend
Lagerung	10 % bis 95 %, nicht kondensierend
Luftdruck	
Betrieb	80 kPa bis 108 kPa, 2000 m ü.N.N.
Lagerung	70 kPa bis 108 kPa, 3000 m ü.N.N.
Einbaulage	senkrecht auf einer Norm-Tragschiene
Verbindung zur Schutzerde	durch Aufrasten auf eine geerdete Tragschiene
Gewicht Kopfstation	1350 g typisch

Versorgungsspannung (US1 / US2 redundant)	
Anschluss	über COMBICON; maximaler Leiterquerschnitt = 2,5 mm^2
Nennwert	24 V DC (SELV)
Zulässiger Spannungsbereich	18,0 V DC bis 32,0 V DC
Prüfspannung	500 V DC für eine Minute
Stromaufnahme an US bei 24 V DC typisch	0,35 ... 3,25 A, abhängig von Konfiguration (Erweiterungen / Interface-Module)
Leistungsaufnahme typisch	8,4 W ... 78 W, abhängig von Konfiguration (Erweiterungen / Interface-Module); siehe Beispiel auf Seite 12-5

Schnittstellen an der Kopfstation	
Anzahl der Steckplätze für Interface-Module	4
Anschlussmedium	über Interface-Module, flexible Medienunterstützung
Anzahl der Ethernet-Ports	
Kopfstation	8
Kopfstation und ein Erweiterungsmodul	16
Kopfstation und zwei Erweiterungsmodule	24
Systemschnittstelle für Erweiterungsmodul	
Anzahl der Erweiterungsmodule	2
Übertragene Signale	Versorgungsspannung, Steuersignale, Daten
V.24-Kommunikationsschnittstelle	
Anschlussformat	Mini-DIN-Buchse
Potenzialfreier Meldekontakt	
Spannung	24 V DC
Stromtragfähigkeit	100 mA maximal

Schnittstellen an den Erweiterungsmodulen	
Anzahl der Steckplätze für Interface-Module	4
Anschlussmedium	über Interface-Module, flexible Medienunterstützung
Anzahl der Ethernet-Ports	8
Systemschnittstelle für Erweiterungsmodul	Ankommende und weiterführende Systembusschnittstelle
Übertragene Signale	Versorgungsspannung, Steuersignale, Daten

RJ45-Schnittstellen (Standard)	
Anzahl	2
Anschlussformat	8-polige RJ45-Buchse am Switch
Anschlussmedium	Twisted-Pair-Leitung mit einem Leiterquerschnitt von 0,14 mm^2 bis 0,22 mm^2
Leitungsimpedanz	100 Ohm
Übertragungsrate	10/100 MBit/s
Maximale Netzsegment-Ausdehnung	100 m

RJ45-Schnittstellen Power over Ethernet IEEE 802.3af	
Anzahl	2
Anschlussformat	8-polige RJ45-Buchse am Switch
Anschlussmedium	Twisted-Pair-Leitung mit einem Leiterquerschnitt von 0,14 mm^2 bis 0,22 mm^2
Leitungsimpedanz	100 Ohm
Übertragungsrate	10/100 MBit/s
Maximale Netzsegment-Ausdehnung	100 m
Vollständige Konfigurationsunterstützung	ab Firmware-Version 4.0 und ab Systembus-Firmware 5.00 in der Kopfstation und ab Systembus-Firmware 4.00 in den Erweiterungsmodulen
Anschluss der PoE-Versorgung	über COMBICON; maximaler Leiterquerschnitt = 2,5 mm^2
Nennwert	48 V DC (SELV)
Zulässige Spannungsbereiche	45,5 V DC bis 53 V DC

RJ45-Schnittstellen Power over Ethernet IEEE 802.3af (Forts.)	
Prüfspannung	500 V AC für eine Minute
Stromaufnahme an US bei 48 V DC maximal	900 mA
Leistungsaufnahme typisch	40 W

Ethernet-Schnittstelle (SC) Multimode	
Anzahl	2
Anschlussformat	SC-Duplex-Buchse am Switch
Wellenlänge	1300 nm
Laserschutz	Klasse 1 nach DIN EN 60825-1:2001-11
min. Übertragungslänge inkl. 3 dB Systemreserve	6,4 km Glasfaser m. F-G 50/125 0,7 dB/km F1200 2,8 km Glasfaser m. F-G 50/125 1,6 dB/km F800 10 km Glasfaser m. F-G 62,5/125 0,7 dB/km F1000 3,0 km Glasfaser m. F-G 62,5/125 2,6 dB/km F1000
Sendeleistung (Fasertyp) dynamisch (average) im Link-Betrieb	
minimal	-23,5 dBm (50/125 µm) / -20 dBm (62,5/125 µm)
maximal	-14 dBm (50/125 µm) / -14 dBm (62,5/125 µm)
Sendeleistung (Fasertyp) statisch	
minimal	-20,5 dBm (50/125 µm) / -17 dBm (62,5/125 µm)
maximal	-11 dBm (50/125 µm) / -11 dBm (62,5/125 µm)
Empfängerempfindlichkeit min.	-31 dBm (dynamisch) / -28dBm (statisch)
Übersteuerungsgrenze max.	-14 dBm (dynamisch) / -11 dBm (statisch)
Übertragungsrate	100 MBit/s

Ethernet-Schnittstellen (SC) Singlemode	
Anzahl	2
Anschlussformat	SC-Duplex-Buchse am Switch
Wellenlänge	1300 nm
Laserschutz	Klasse 1 nach DIN EN 60825-1:2001-11
min. Übertragungslänge inkl. 3 dB Systemreserve	36 km Glasfaser m. F-G 9/125 0,36 dB/km 32 km Glasfaser m. F-G 9/125 0,4 dB/km 26 km Glasfaser m. F-G 9/125 0,5 dB/km
Sendeleistung (Fasertyp) dynamisch (average) im Link-Betrieb	
minimal	-15,0 dBm (9/125 µm)
maximal	-8,0 dBm (9/125 µm)
Empfängerempfindlichkeit min.	>-31 dBm (9/125 µm)
Übersteuerungsgrenze max.	>-7 dBm (9/125 µm)
Übertragungsrate	100 MBit/s

Ethernet-Schnittstellen POF-SMA	
Anzahl	1 (FL IF TX/POF 100...) 2 (FL IF 2POF 100...)
Anschlussformat	F-SMA-Buchsen am Interface-Modul
Datenübertragungsrate	10/100 MBit/s
Wellenlänge	650 nm
Minimale Leitungslänge	1 m
Übertragungslänge inkl. 3 dB Systemreserve	50 m Polymerfaser mit F-K 980/1000 230 dB/km

Ethernet-Schnittstellen POF-SMA (Forts.)	
Sendeleistung (Fasertyp) dynamisch im Link-Betrieb (average)	
Minimum	-8,0 dBm (980/1000 µm) -12 dBm (980/1000 µm) per Schalter abgesenkt
Empfängerempfindlichkeit (Fasertyp) dynamisch im Link-Betrieb (average)	
Minimum	-23,0 dBm (980/1000 µm)
Optische Übersteuerungsgrenze	-11,5 dBm (980/1000 µm)

Ethernet-Schnittstellen HCS	
Anzahl	2
Anschlussformat	F-SMA-Buchsen am Interface-Modul
Datenübertragungsrate	100 MBit/s
Wellenlänge	650 nm
Übertragungslänge inkl. 3 dB Systemreserve	100 m HCS-Faser mit F-S 200/230 10 dB/km
Sendeleistung (Fasertyp) dynamisch im Link-Betrieb (average)	
Minimum	-13 dBm (200/230 µm)
Empfängerempfindlichkeit (Fasertyp) dynamisch im Link-Betrieb (average)	
Minimum	-23,0 dBm (200/230 µm)
Optische Übersteuerungsgrenze	-11,5 dBm (200/230 µm)

Ethernet-Schnittstellen SCRJ mit optischer Diagnose	
Anzahl	2 (FL IF 2POF SCRJ-D)
Anschlussformat	SC-RJ-Buchsen am Interface-Modul
Datenübertragungsrate	10/100 MBit/s (100 MBit/s nach PROFINET-Standard)
Wellenlänge	660 nm
Laserschutz	Klasse 1 nach DIN EN 60825-1
Minimale Leitungslänge	1 m
Übertragungslänge inkl. 3 dB Systemreserve	max. 50 m Polymerfaser mit F-K 980/1000 230 dB/km bei 10/100 MBit/s max. 100 m HCS-Faser mit F-S 200/230 8 dB/km bei 100 MBit/s
Sendeleistung (Fasertyp) dynamisch im Link-Betrieb (average)	
Minimum	-8,0 dBm (980/1000 µm)
Empfängerempfindlichkeit (Fasertyp) dynamisch im Link-Betrieb (average)	
Minimum	-23,0 dBm (980/1000 µm)
Optische Übersteuerungsgrenze	1,0 dBm (980/1000 µm)

Leitungslängen	
Twisted Pair	100 m
Polymerfaser - POF	abhängig vom Interface-Modul minimal 1 m
HCS	abhängig vom Interface-Modul
Glasfaser 1300 nm (Multimode)	6400 m mit Glasfaser mit F-G 50/125 0,7 dB/km F1200 2800 m mit Glasfaser mit F-G 50/125 1,6 dB/km F800 10000 m mit Glasfaser mit F-G 62,5/125 0,7 dB/km F1000 3000 m mit Glasfaser mit F-G 62,5/125 2,6 dB/km F600
Glasfaser 1300 nm (Singlemode)	36000 m mit Glasfaser mit F-G 9/125 0,36 dB/km 32000 m mit Glasfaser mit F-G 9/125 0,4 dB/km 26000 m mit Glasfaser mit F-G 9/125 0,5 dB/km

Mechanische Prüfungen	
Schockprüfung nach IEC 60068-2-27	Betrieb: 25g, 11 ms Dauer, Halbsinus-Schockimpuls Lagerung/Transport: 50g, 11 ms Dauer, Halbsinus-Schockimpuls
Vibrationsfestigkeit nach IEC 60068-2-6	Betrieb/Lagerung/Transport: 5g, 10 - 150 Hz, Kriterium 3
Freier Fall nach IEC 60068-2-32	1 m

Konformität zu EMV-Richtlinien	
Störaussendung nach EN 55011	Klasse A
Warnung: Die Grenzwerte der gestrahlten elektromagnetischen Störaussendung gemäß EN 55011, Klasse A werden von dem Modul nur eingehalten, wenn es in einem geerdeten metallischen Schaltschrank installiert ist.	
Funkstörfeldstärken nach EN 55022	Klasse A
Statische Entladung (ESD) nach EN 61000-4-2	Klasse 3; Kriterium B
Elektromagnetische Felder nach IEC 61000-4-3	10 V/m; Kriterium A
Leitungsgebundene Störungen nach IEC 61000-4-6	10 V_{RMS}; Kriterium A
Schnelle Transienten (Burst) nach IEC 61000-4-4	Data-Lines: 1 kV; Kriterium A Power-Supply-Lines: 2,2 kV; Kriterium B
Stoßspannungen (Surge) nach IEC 61000-4-5	Data-Lines: ± 1 kV unsym.; Kriterium B Power-Supply-Lines: ± 0,5 kV sym./unsym.; Kriterium B

Unterschiede zu vorhergehenden Versionen
Rev. 01: Kapitel „Spanning Tree“ eingefügt; FL IF 2FX SM ... eingefügt
Rev. 02: Technische Daten der POF-Schnittstelle eingefügt
Rev. 03: Multicast-Filtering eingefügt, Daten zu den Interface-Modulen überarbeitet
Rev. 04: Extended Multicast-Filtering eingefügt, Handlings-Verbesserung beim Memory Modul beschrieben
Rev. 05: VLAN und RSTP eingefügt, sowie neue Interface-Module und die GL-Zertifizierung
Rev. 06: Ergänzung zu Environmental Category 1 eingefügt
Rev. 07/8: Funktionen und Neuerungen der Firmware-Version 4.0 und Interface-Module ergänzt
Rev. 09: Funktionen und Neuerungen der Firmware-Version 4.50 und Interface-Module sowie Zubehör ergänzt
Rev. 10: Funktionen und Neuerungen der Firmware-Version 4.60 und MRP-Interface-Modul ergänzt

12.2 Typische Stromaufnahme - MMS (Beispiel)

Typische Stromaufnahme der Module	
FL SWITCH MM HS [1]	350 mA
FL MXT [2]	250 mA
FL IF 2TX VS-RJ ... [3]	0 mA
FL IF 2HCS 100 ... [4]	100 mA
FL IF 2FX (SM) SC oder ST ... [5]	200 mA
FL IF TX/POF 10/100 ... [6]	60 mA
FL IF TX/HCS 100 ... [7]	60 mA
FL IF MEM ... [8]	0 mA
FL IF 2PSE ...	30 mA (aus MMS, zusätzlich maximal 850 mA aus der externen 48-V-PoE-Versorgung

Typische Stromaufnahme der Module (Forts.)	
FL IF 2POF SCRJ-D	200 mA

Aufbaubeispiele

Station mit 2 FX-Modulen und 2 TX-Modulen
350 mA [1]+ (2 x 200 mA [5]) + (2 x 0 mA [3])= 750 mA

Station mit 2 FX-Modulen, 5 HCS-Modulen und 1 POF/TX-Modul
350 mA [1] + 250 mA [2] + (2 x 200 mA [5]) + (5 x 100 mA [4]) + 60 mA [6] = 1560 mA

Station mit 5 FX-Modulen, 4 HCS-Modulen, 2 TX-Modulen und 1 POF/TX-Modul
350 mA [1] + (2 x 250 mA [2]) + (5 x 200 mA [5]) + (4 x 100 mA [4]) + (2 x 0 mA [3]) + 60 mA [6] = 2310 mA

12.3 Bestelldaten

Produkte

Beschreibung	Artikel-Bezeichnung	Artikel-Nr.	VPE
Modularer Switch mit Management - Kopfstation	FL SWITCH MM HS	2832328	1
Erweiterungsmodul mit vier Steckplätzen für acht Ports	FL MXT	2832331	1
Konfigurationskabel, Kopplung des Switches mit einem PC, RS 232	PRG CAB MINI DIN	2730611	1
Universal-Endhalter	E/NS 35 N	080088 6	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **vorn**	FL IF 2TX VS-RJ-F	2832344	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **unten**	FL IF 2TX VS-RJ-D	2832357	1
Interface-Modul mit 2 × Glasfaser (Multimode) 100 MBit/s im SC-Format mit Anschlussrichtung von **vorn**	FL IF 2FX SC-F	2832412	1
Interface-Modul mit 2 × Glasfaser (Multimode) 100 MBit/s im SC-Format mit Anschlussrichtung von **unten**	FL IF 2FX SC-D	2832425	1
Interface-Modul mit 2 × Glasfaser (Multimode) 100 MBit/s im ST/BFOC-Format mit Anschlussrichtung von **unten**	FL IF 2FX ST-D	2884033	1
Interface-Modul mit 2 × Glasfaser (Singlemode) 100 MBit/s im SC-Format mit Anschlussrichtung von **vorn**	FL IF 2FX SM SC-D-F	2832205	1
Interface-Modul mit 1 × Twisted Pair 10/100 MBit/s im RJ45-Format und 1 × Polymerfaser 10/100 MBit/s im F-SMA-Format mit Anschlussrichtung von **unten**	FL IF TX/POF 10/100-D	2832807	1
Interface-Modul mit 1 × Twisted Pair 10/100 MBit/s im RJ45-Format und 1 × HCS-Faser 100 MBit/s im F-SMA-Format mit Anschlussrichtung von **unten**	FL IF TX/HCS 100-D	2832739	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **unten** und **Parametrierungsspeicher**	FL IF MEM 2TX-D	2832483	1
Interface-Modul mit 2 × Polymerfaser 10/100 MBit/s im F-SMA-Format mit Anschlussrichtung von **unten**	FL IF 2POF 10/100-D	2832852	1
Interface-Modul mit 2 × HCS-Faser 100 MBit/s im F-SMA-Format mit Anschlussrichtung von **unten**	FL IF 2HCS 100-D	2832742	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format und **Power over Ethernet** mit Anschlussrichtung von **vorn**	FL IF 2PSE-F	2832904	1
Interface-Modul mit 2 × Polymerfaser 10/100 MBit/s im SC-RJ-Format mit Anschlussrichtung von **unten** und **optischer Diagnose**	FL IF 2POF SCRJ-D	2891084	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **unten** und **Parametrierungsspeicher** sowie der **MRP-Lizenz**	FL IF MEM 2TX-D/MRM	2891770	1

Zubehör

Beschreibung	Artikel-Bezeichnung	Artikel-Nr.	VPE
Converter Board, mit dem das Interface-Modul FL IF TX/POF 100... zu einem „Stand-Alone-Medienkonverter“ erweitert werden kann	FL CB IF	2832470	1
Beschriftungsfeld zur Kennzeichnung der Ports von Kopstation und Erweiterungsmodulen	FL M LABEL	2891055	1
RJ45-Stecker mit zusätzlicher Verrastung	VS-08-T-G-RJ45/IP20	1652295	5
RJ45-Steckerset **grau** für Geradeaus-Leitung	FL PLUG RJ45 GR/2	2744856	2
RJ45-Steckerset **grün** für gekreuzte Leitung	FL PLUG RJ45 GN/2	2744571	2
Konfektionierungs-Zange für RJ45-Stecker	FL CRIMPTOOL	2744869	1
Inbetriebnahme/Diagnose-Software „Factory Manager“	FL SWT	2831044	1
Netzwerküberwachung mit HMI/SCADA-Systemen	FL SMNP OPC SERVER	2832166	1
Patchbox 8 x RJ45 CAT5e vorbestückt, nachrüstbar	FL PBX 8TX	2832496	1
Patchbox 6 x RJ45 CAT5e und 4 SC-RJ glas vorbestückt, nachrüstbar	FL PBX 6TX/4FX	2832506	1

Beschreibung (Forts.)	Artikel-Bezeichnung	Artikel-Nr.	VPE
Patchwinkel mit zwei RJ45-Netzwerkanschlüssen CAT5e inklusive Layer-1-Security-Elementen	FL PF SEC 2TX	2832687	1
Patchwinkel mit acht RJ45-Netzwerkanschlüssen CAT5e inklusive Layer-1-Security-Elementen	FL PF SEC 8TX	2832690	1
Patchwinkel mit zwei RJ45-Netzwerkanschlüssen CAT5e	FL PF 2TX CAT5E	2891165	1
Patchwinkel mit acht RJ45-Netzwerkanschlüssen CAT5e	FL PF 8TX CAT5E	2891178	1
Patchwinkel mit zwei RJ45-Netzwerkanschlüssen CAT6	FL PF 2TX CAT 6	2891068	1
Patchwinkel mit acht RJ45-Netzwerkanschlüssen CAT6	FL PF 8TX CAT 6	2891071	1
Patchkabel, CAT 5, vorkonfektioniert, 0,3 m lang	FL CAT5 PATCH 0,3	2832250	10
Patchkabel, CAT 5, vorkonfektioniert, 0,5 m lang	FL CAT5 PATCH 0,5	2832263	10
Patchkabel, CAT 5, vorkonfektioniert, 1,0 m lang	FL CAT5 PATCH 1,0	2832276	10
Patchkabel, CAT 5, vorkonfektioniert, 1,5 m lang	FL CAT5 PATCH 1,5	2832221	10
Patchkabel, CAT 5, vorkonfektioniert, 2,0 m lang	FL CAT5 PATCH 2,0	2832289	10
Patchkabel, CAT 5, vorkonfektioniert, 3,0 m lang	FL CAT5 PATCH 3,0	2832292	10
Patchkabel, CAT 5, vorkonfektioniert, 5,0 m lang	FL CAT5 PATCH 5,0	2832580	10
Patchkabel, CAT 5, vorkonfektioniert, 7,5 m lang	FL CAT5 PATCH 7,5	2832616	10
Patchkabel, CAT 5, vorkonfektioniert, 10,0 m lang	FL CAT5 PATCH 10	2832629	10
Polymerfaser-Stecker (zwei Duplex-Stecker im Set)	PSM-SET-SCRJ-DUP/2-POF	2708656	1
Polierset für Polymerfaser-Stecker (erforderlich zur Montage der Polymerfaser-Stecker)	VS-SCRJ-POF-POLISH	1656673	1
LWL-Polymerfaser-Kabel für die Innenverlegung	PSM-LWL-KDHEAVY	2744319	1
HCS-Faser-Stecker (zwei Duplex-Stecker im Set)	PSM-SET-SCRJ-DUP/2-HCS	2313070	1
Werkzeug-Set für HCS-Stecker (erforderlich zur Montage der HCS-Faser-Stecker	PSM-HCS-KONFTOOL/SCRJ	2708876	1
LWL-HCS-Kabel für die Innenverlegung	PSM-LWL-HCS-RUGGED-200/230	2799885	1
LWL-HCS-Kabel für die Außenverlegung	PSM-LWL-HCSO-200/230	2799445	1

12.4 Bestelldaten der nach GL zertifizierten Komponenten (GL-Zertifikat 24 2750 4 HH)

Produkte

Beschreibung	Artikel-Bezeichnung	Artikel-Nr.	VPE
Modularer Switch mit Management - Kopfstation	FL SWITCH MM HS/M	2832522	1
Erweiterungsmodul mit 4 Steckplätzen für acht Ports	FL MXT/M	2832535	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **unten** und **Parametrierungsspeicher**	FL IF MEM 2TX-D	2832483	1
Interface-Modul mit 2 × Glasfaser (Multimode) 100 MBit/s im SC-Format mit Anschlussrichtung von **unten**	FL IF 2FX SC-D	2832425	1
Interface-Modul mit 2 × Glasfaser (Singlemode) 100 MBit/s im SC-Format mit Anschlussrichtung von **unten**	FL IF 2FX SM SC-D	2832205	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **vorn**	FL IF 2TX VS-RJ-F	2832344	1
Interface-Modul mit 2 × Twisted Pair 10/100 MBit/s im RJ45-Format mit Anschlussrichtung von **unten**	FL IF 2TX VS-RJ-D	2832357	1

HOTLINE:

Bei Problemen, die nicht mit Hilfe dieser Dokumentation gelöst werden können, wenden Sie sich bitte an unsere Hotline:

+ 49 - (0) 52 35 - 3-4 18 88

factoryline-service@phoenixcontact.com

A Anhang: Stichwortverzeichnis

Symbols

%-Skala 4-38

Numerics

0.x.x.x-Adressen 3-4
127.x.x.x-Adressen 3-4
48-V-Versorgung 3-24
7-Segment-Anzeige 1-14

A

abgeschaltetem Port 4-27
Ablaufdiagramm
Vergabe der IP-Parameter 3-8
Ablaufdiagramm nach Neustart 3-7
Access Control 4-19
Access Control for Web 4-20
Adressen lernen 3-30
Adresskombinationen 3-3
Agent 4-42
Aging Time 4-32
Aging-Time 3-1
Allowed MAC Address 4-33
Alternate-Port 5-27
Analyse-Möglichkeit 4-40
Anschluss der 48-V-PoE-Versorgungsspannung 3-25
Anschluss der F-SMA-Stecker 3-12
Anschluss der RJ45-Stecker 3-10
Anschluss der SC-D-Stecker 3-17, 3-28
Anschluss der ST-Stecker 3-18
Aufbau der Netzmaske 3-4
Auslieferungszustand 3-1
Auslieferungszustand des Parametrierungsspeichers 3-22
Autocrossing 3-9
Autonegotiation 3-9
Autopolarity 3-9

B

Balkendiagramm 4-38
Basic Switch Configuration 4-124
Baumstruktur 5-1
Baumstruktur der MIB 4-45
Bearbeitungsregeln 3-31
Belegung der RJ45-Buchse 3-11
Block Packets 4-33
Block Packets with automatic reenabling 4-33
Blockade 4-34
BootP 4-14
BootP-Reply 4-14
Bootstrap Protocol 4-14
BPDU-Pakete 3-31
Bridge-MIB 4-41

C

Cascading Style Sheets Level 1 4-11
Change Password 4-18
Class 0 4-35
Class 4 4-35
Clear Memory Module 4-24
Configuration com parison 4-24
Converter Board 1-4
CRC-Fehler 3-30
Ctrl + L 4-122

D

Datenbits 2-12
DCP 4-15
Default Priorität 3-31
defekter Firmware 4-126
defekter Software 4-126
Demontage 2-3
Designated-Port 5-26
Destination-Port 4-32
DHCP 4-15
DHCP-Lease-Time 3-8
DHCP-Server 3-8
Diagnose/Status-Anzeigen 1-7
DIP-Schalter 3-13
Disconnected Load 3-24
Discovery and Configuration Protocol 4-15
Diskettensymbol 4-11
Display 4-36
Dotted Decimal Notation 3-3
Dotted-Notation 4-19
Download der Firmware 4-17
Dynamic Host Configuration Protocol 4-15

E

Edge-Port 5-27
Einsatz des VS-08-T-G-RJ45/IP20 3-10
EMC1 2-10
Empfangs-Queue 3-31
Endgeräte 4-33
Engineering-Werkzeug 4-15
Environmental Category EMC2 2-10
Erdung 2-12
Erforderliche Hardware 1-7
Erweiterungsmodul 1-4
Etherlike-MIB 4-41
Event Table 4-38
Excell-Tabelle 4-40
externes Management 2-12

F

Factory Manager 4-1
Far-End-Fault-Detection 3-16, 3-18, 3-27
Faseranschluss 3-15
Fasertyp 3-17, 3-28
Fehler-Code „87“ 3-22
Fehlerzustände 2-11
Firmware-Update 4-7
Firmware-Versionen 1-5
FL IF 2FX SC 3-16, 3-27
FL IF 2FX SM SC 3-16
FL IF 2FX ST-D 3-18
FL IF 2HCS 100 3-14
FL IF 2POF 10/100 3-11
FL IF 2PSE-F 3-24
FL IF 2TX VS-RJ 3-9
FL IF MEM 2TX-D 3-22
FL IF TX/HCS 100 3-20
FL IF TX/POF 10/100 3-19
FL MXT/M 1-1
FL SWITCH MM HS/M 1-1
Flusssteuerung 2-12
Forward Delay 5-5
Fragmente 3-30
Frame-Switching 3-30
Frontansicht 1-8
F-SMA-Port 3-11
Funktion des Memory-Moduls 3-22
Funktionsumschalter 1-7

G

Gerätetausch 4-23
GL 1-3
GL zertifizierten Betrieb 3-9
Glasfaser-Verbindung 3-17, 3-28
GL-zertifizierten Betrieb 2-10
Gültige IP-Parameter 3-2

H

HCS-Port 3-14
HCS-Verbindung 3-15
Hello Time 5-5
Host-ID 3-3
Hot-Plugging 2-5
Hyper Text Transfer Protocol 4-11
Hyperterminal 4-126
Hyperterminals 4-122

I

Iana-address-family-MIB 4-41
IANAifType-MIB 4-41
IEEE 802.1D 3-31
IEEE 802.1d 5-1
IEEE 802.1w 5-1
IEEE 802.3 3-11
If-MIB 4-41
IGMP-Pakete 3-31
Illegal Address Counte r 4-25
illegalen Zugriffe 4-32
Industrietauglicher RJ45-Stecker 3-10
IO-Controller 4-15
IP-Adresse 3-1
IP-Adressvergabe 4-14
IP-Sonderadressen 3-4

J

Javascript 1.2 4-11

K

Konfiguration beim Booten 4-23
Konfigurationsdatei 4-22
Konfigurations-Vergleich 4-24

L

Laden der Konfigurationsdaten ... 3-7
Large Tree Support ... 5-5
Last Source MAC Address ... 4-34
LEDs ... 1-12
Leitungsüberwachung ... 3-10
Leitungsunterbrechung ... 3-10
Lese-Schreib-Rechte ... 4-19
Link-Test-Pulse ... 3-10
Link-Überwachung ... 4-26
Load the last stored configuration ... 4-22
Login Screen ... 4-123
Logout ... 4-12

M

Mac Address Table ... 4-40
MAC-Adresse ... 3-30
Management Information Base ... 4-42
Management Informationen Base ... 4-41
Management über lokale V.24-Kommunikationsschnittstelle ... 4-122
Management über Telnet ... 4-129
Maße des Modular Managed Switch System ... 1-10
Maximum Age of STP Information ... 5-5
Meldekontakt ... 2-11
Memory Module ... 4-23
MIB ... 4-41
MIB 2 ... 4-41
Mini-DIN-Buchse ... 2-12
Mini-DIN-Format ... 4-122
Modularer Aufbau ... 1-2
Montage ... 2-3
Multi-/Broadcast-Adresse ... 3-30
Multiadress-Fähigkeit ... 3-30
Multicast-Datenpakete ... 4-32

N

Navigations-Baum ... 4-12
NEF 1- 6 ... 2-10
Netz-ID ... 3-3
Netzklasse ... 3-3
Netz-Verfügbarkeit ... 1-2
Netzwerkteil ... 3-4
Netzwerktopologie ... 5-2
No redundancy ... 5-3
Nur-Lese-Rechte ... 4-19

O

Online Diagnostics ... 4-37

P

Paketabarbeitungsreihenfolge ... 3-31
Parität ... 2-12
Passwort ... 4-11, 4-12
Passwort „private“ ... 4-18
Passwort vergessen ... 4-18
Passwort-Konzept ... 4-12
P-Bridge-MIB ... 4-41
PoE-Interface ... 3-24
PoE-Interface-Modul ... 4-35
PoE-Konfiguration ... 4-35
POF-Interface ... 3-12
POF-Verbindung zwischen Geräten ... 3-12
Polymer-/HCS-Faser ... 1-1
Polymerfaser-LWL-Strecken ... 3-13
Port Cfg. Table ... 4-26
Port Mirroring ... 4-32
Port PoE Table ... 4-34
Port Security ... 4-32
Port Security Status ... 4-24
Port Table ... 4-26
Port-Auslastung ... 4-32
Port-basierende Gewichtung von Datenströmen ... 3-31
Port-Priorisierung ... 3-31
Port-Rollen ... 5-26
Power over Ethernet Port Table ... 4-34
Priorisierung ... 3-31
Prioritätsfeld ... 3-31
Prioritätsstufe ... 3-31
Priority Queues ... 3-31
Private MIBs ... 4-70
PROFINET ... 4-15
PROFINET-Verbindung ... 4-15
Punkt-zu-Punkt-Verbindung ... 4-23
pxcFactoryLine ... 4-70
pxcGlobal ... 4-70
pxcModules ... 4-70

Q

Q-Bridge-MIB ... 4-41

Quell- und Zieladressen 3-30

R

Rapid Reconfiguration Spanning Tree 5-1
Rapid Spanning Tree Protocol 5-1
Rastlaschen 2-3
Reboot 4-24
Redundante 24-V-DC-Einspeisung 2-9
redundanten Datenpfaden 5-1
Redundanz-Mechanismus 5-2
Refresh Intervall 4-18
Request 4-14
RFC1213 4-41
RFC1213-MIB 4-46
RMON-MIB 4-41
Root 5-1
Root-Port 5-26
RSTP-MIB 4-41
Rücksetzen auf Werkseinstellungen 4-125, 4-131

S

Save current configuration 4-21
Schalterstellung 3-13
Schiffsbau 1-3
Schutzkappen 3-14
Security Mode 4-32
Sendeleistung 3-13
Set default upon delivery 4-21
Simple Network Management Protocol 4-41
SNMP 4-41
SNMP-FRAMEWORK-MIB 4-41
SNMP-Interface 4-41
SNMP-Objekte 4-41
SNMPv2-MIB 4-41
Software Update 4-17
Source-Port 4-32
Speichern der Firmware 4-17
Standard-Browsers 4-11
Start mit defekter Software 4-126
Stati von „Status of current configuration“ 4-21
Static Assignment 4-14
Staubschutzkappen 3-14
Stoppbits 2-12
Store-and-Forward-Modus 3-30
STP 5-1
Strict Priority 3-32
Subnetzmaske 3-1
Subnetzmasken 3-4
Subnetzrouter 3-5
Switch Station 4-24
Systembusfirmware 3-22

T

Tagging 3-32
Telnet-Client 4-129
Telnet-Protokoll 4-129
Telnet-Server 4-129
Telnet-Terminals 4-129
Terminal-Emulation 2-12
TFTP Server 4-7
Thermischer Fehler 3-24
Traffic Classes 3-31, 3-32
Trap Configuration 4-16
Trap only 4-32
Trap- Receiver 4-16
Traps 4-42
Trap-Targets/Receiver 4-42

U

Überlast 3-24
Überspannung/Unterspannung 3-24
unberechtigten Zugriffe 4-25
UND-Verknüpfung 3-5
Unicast-Adressen 3-31
User Interfaces 4-18
User-Interface 4-130
User-Interfaces 4-123
Utilization 4-38

V

V.24-Schnittstelle 2-12
Vergabe der IP-Parameter 3-2
Vergabe von IP-Adressen 3-2
Versorgungsspannung 2-9
VLAN-/Prioritäts-Tag 3-31
VLAN-ID 4-40
VS-08-T-G-RJ45/IP20 3-10
VT100-Terminal 2-12

W

WBM 4-11

Web Based Management 4-11
Webserver 4-11
Werkseinstellungen 3-1
Wurzel..... 5-1

X

XMODEM-Bereitschaft 4-127

Z

Zählerstände..... 4-29
Zieladresse 3-30
Zieladressfeld 3-30
Zuordnung der F-SMA-Ports 3-13
Zuordnung der Ports..... 1-11